Ruijie RG-CS86 Series Switches

CS86_RGOS 12.6(2)B0103

Configuration Guide

Document Version: V1.0
Date: 2023.04.27
Copyright © 2023 Ruijie Networks

Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Trademark Ruijie Networks 锐捷 and Ruijie are owned by Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Live Chat: https://www.ruijienetworks.com/rita

Conventions

1. Conversions

Convention	Description
Bold font	Commands, command options, and keywords are in **bold** font.
Italic font	Arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
&<1-n>	The argument before the sign (&) can be input for consecutive 1- n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

2. Signs

The signs used in this document are described as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

3. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

Basic Configuration

1. CLI Configuration
2. ZAM Configuration
3. Basic Management Configuration
4. RBAC Configuration
5. Line Configuration
6. File System Configuration
7. HTTP Configuration
8. Syslog Configuration
9. Software Upgrade Configuration
10. Time Range Configuration
11. Supervisor Module Redundancy Configuration
12. Hot Swapping Configuration
13. Process Restarting Configuration
14. Python Configuration
15. Software License Management Configuration
16. USB Configuration

Contents

1 Configuring the CLI 1
1.1 Introduction 1
1.1.1 Accessing the CLI 1
1.1.2 Command Modes 1
1.1.3 System Help 3
1.1.4 Abbreviated Commands 4
1.1.5 No and Default Options of Commands 4
1.1.6 Prompts for Incorrect Commands 5
1.1.7 History Commands 5
1.1.8 Featured Editing 6
1.1.9 Searching and Filtering of the Show Command Output 7
1.1.10 Command Alias 8
1.1.11 Character Set Encoding 9
1.2 Restrictions and Guidelines 9
1.3 Configuration Task Summary 10
1.4 Operating the Python Script 10
1.5 Configuring a Command Alias 10
1.6 Configuring the Privilege Level of a Command 11
1.7 Configuring the Character Set Encoding Format 11
1.8 Monitoring 11

1 Configuring the CLI

1.1 Introduction

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

1.1.1 Accessing the CLI

Before using the CLI, you need to connect a terminal or PC to a network device. After you start the network device and initialize the hardware and software of the network device, you can use the CLI. If you use the network device for the first time, you can connect it only through the console port. This is called out-of-band management. After performing relevant configuration, you can connect and manage the network device by telnetting to the virtual terminal.

1.1.2 Command Modes

Since the device has many commands, you can classify them by function to facilitate their use. The CLI provides several commands modes, and all commands are registered in one or several command modes. You must enter the mode of a command before using this command. Command modes are related with each other but differ from each other.

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

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

Using commands in configuration modes (such as global configuration mode and interface configuration mode) affects configurations in use. If you save the configurations, these commands are saved and run when the system restarts. To enter another configuration mode, enter global configuration mode. If you perform configuration in global configuration mode, you can enter various configuration sub-modes, such as interface configuration mode.

Table 1-1 Description of the Command Modes (suppose that the name of the network device is "Ruijie")

Command Mode	Access Method	Prompt	Exit or Entering Next Mode	Function Description of the Mode
User EXEC mode	A user enters user EXEC mode by default when accessing a network device.	Ruijie>	● Run the **exit** command to exit this mode. ● Run the **enable** command to enter privileged EXEC mode.	Use this command mode to conduct basic tests or display system information.
Privileged EXEC mode	In User EXEC mode, run the **enable** command to enter privileged EXEC mode.	Ruijie#	● Run the **disable** command to return to user EXEC mode. ● Run the **configure** command to enter global configuration mode.	Use this command mode to check whether the configurations take effect. This mode is password-protected.
Global configuration mode	In Privileged EXEC mode, run the **configure** command to enter global configuration mode.	Ruijie(config)#	● Run the **exit** or **end** command, or press **Ctrl+C** to return to privileged EXEC mode. ● Run the **interface** command to enter interface configuration mode. In the **interface** command, you must specify the interface configuration sub-mode you want to enter. ● Run the **vlan** *vlan-id* command to enter VLAN configuration mode.	Use commands in this mode to configure global parameters that affect the entire network device.
Interface configuration mode	In global configuration mode, run the **interface** command to enter interface configuration mode.	Ruijie(config-if)#	● Run the **end** command or press **Ctrl+C** to return to privileged EXEC mode. ● Run the **exit** command to return to global configuration mode. In the **interface** command, you must specify the interface configuration sub-mode you want to enter.	Use this command mode to configure various interfaces of the network device.

Command Mode	Access Method	Prompt	Exit or Entering Next Mode	Function Description of the Mode
Config-vlan (VLAN configuration mode)	In global configuration mode, run the **vlan** *vlan-id* command to enter VLAN configuration mode.	Ruijie(config-vlan)#	• Run the **end** command or press **Ctrl+C** to return to privileged EXEC mode. • Run the **exit** command to return to global configuration mode.	Use this command mode to configure VLAN parameters.

1.1.3 System Help

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

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

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

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

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

```
  range           Interface range command
```

Note

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

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

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

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

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

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

- In any command mode, you can run the **help** command to obtain brief description of the help system.

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

1.1.4 Abbreviated Commands

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

For example, the **interface gigabitEthernet 0/1** command for entering the configuration mode of interface GigabitEthernet 0/1 is abbreviated as follows:

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

1.1.5 No and Default Options of Commands

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

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

Note

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

1.1.6 Prompts for Incorrect Commands

If an incorrect command is entered, an error prompt is displayed.

Table 1-2 Common CLI Errors

Error	Description	How to Obtain Help
% Ambiguous command: "show c"	The characters entered are too few to identify a unique command.	Enter the command again, and enter a question mark (?) after the ambiguous word. All the possible keywords are displayed.
% Incomplete command.	The mandatory keyword or variable is not entered in the command.	Enter the command again, and enter a space and a question mark (?). All the possible keywords or variables are displayed.
% Invalid input detected at '^' marker.	An incorrect command is entered. The symbol (^) indicates the position of the wrong word.	At the current command mode prompt, enter a question mark (?). All the command keywords allowed in this command mode are displayed.

1.1.7 History Commands

The system automatically saves commands that are entered recently. You can use shortcut keys to query or call history commands.

Table 1-3 Operation Methods

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

Specification

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

1.1.8 Featured Editing

When editing commands, you can use the keys or shortcut keys listed in the following table:

Table 1-4 Description of Shortcut Keys

Function	Key or Shortcut Key	Description
Move the cursor in a line.	Left key or Ctrl+B	Move the cursor to the left by one character.
	Right key or **Ctrl**+**F**	Move the cursor to the right by one character.
	Ctrl+**A**	Move the cursor to the head of the command line.
	Ctrl+**E**	Move the cursor to the end of the command line.
Delete an entered character.	Backspace key	Delete one character to the left of the cursor.
	Delete key	Delete one character to the right of the cursor.
Move the output by one line or one page.	Enter key	When the output is displayed, press the **Enter** key to move the output one line upward and display the next line. Use this key only when the output does not end yet.
	Space key	When the output is displayed, press the **Space** key to page down and display the next page. Only when the output does not end, use this key.

When the cursor is close to the right boundary, the entire command line moves to the left by 20 characters, and the hidden front part is replaced with a dollar ($) sign. You can use related keys or shortcut keys to move the cursor to the characters in the front or return to the head of the command line.

For example, the entire **access-list** command may be wider than the screen. When the cursor is first close to the end of the command line, the entire command line moves to the left by 20 characters, and the hidden front part is replaced with a dollar sign ($). Each time the cursor is close to the right boundary, the entire command line moves to the left by 20 characters.

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

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

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

Note

The default line width of terminals is 80 characters.

1.1.9 Searching and Filtering of the Show Command Output

- To search specified content in the output of the **show** command, run the following command:

Table 1-5 Searching for Specified Content in the Output of the show Command

Command	Purpose
show *any-command* | [**regexp**] **begin** *regular-expression*	Searches for specified content in the output of the **show** command, and outputs the first line containing the content and all information that follows this line.

- To filter specified content in the output of the **show** command, run the following commands:

Table 1-6 Filtering Specified Content in the Output of the show Command

Command	Purpose
show *any-command* | [**regexp**] **exclude** *regular-expression*	Filters the output of the **show** command to filter out lines containing the specified content, and outputs other information.
show *any-command* | [**regexp**] **include** *regular-expression*	Filters the output of the **show** command to output only the lines containing the specified content, and filters out other information.

Note

- The **show** command can be executed in any mode.
- Searched content is case-sensitive.

When the **regexp** keyword is specified, a regular expression can be used for filtering content. The following table describes the usages of special characters in a regular expression.

Table 1-7 Description of Usages of Special Characters in a Regular Expression

Character	Symbol	Special Meaning
Period	.	Matches any single character.
Plus sign	+	Matches one or any sequence in a string.
Caret	^	Matches the start of a string.
Underline	_	Matches commas, brackets, start and end of a string, and spaces.
Square brackets	[ ]	Matches a single character within a range.

To search or filter the output of the **show** command, you must enter a vertical line (|). After the vertical line, specify the search or filter rules and content to be searched or filtered (characters or strings). Content to be searched and filtered is case-sensitive.

```
Ruijie# show running-config | include interface
interface GigabitEthernet 0/0
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
interface GigabitEthernet 0/4
interface GigabitEthernet 0/5
interface GigabitEthernet 0/6
interface GigabitEthernet 0/7
interface Mgmt 0
Ruijie# show running-config | regexp include GigabitEthernet [0-9]/1
interface GigabitEthernet 0/1
```

1.1.10 Command Alias

You can specify any word as the alias of a command to simplify the input of the command string.

1. Default aliases in the system

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

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

Note

Default aliases in the system cannot be deleted.

2. System help regarding command aliases

- The system provides help information for command aliases. An asterisk (*) is displayed in front of an alias in the following format:

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

For example, in privileged EXEC mode, the default command alias "s" represents the keyword **show**. If you enter "s?", help information of the keywords and aliases starting with "s" is displayed.

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

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

For example, in privileged EXEC mode, configure the alias "sv" to replace the **show version** command. If you enter "s?", help information of the keywords and aliases starting with "s" is displayed.

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

- You can use an alias to obtain help information of the command represented by the alias.

For example, if you configure the alias "ia" in interface configuration mode to represent the **ip address** command, you can enter "ia?" in interface configuration mode to obtain help information of "**ip address**?", and replace the alias with the actual command.

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

Caution

If you enter a space in front of a command alias, the command represented by this alias is displayed.

1.1.11 Character Set Encoding

The function of character set encoding enables the device to use a unified character set encoding format by configuring character set encoding. After a command is entered in the CLI of a terminal, the command is automatically converted into a command in the unified character set encoding format before delivery.

Note

When hybrid formats exist in current running configurations, you must manually delete running configurations containing the encoding format different from the target format before modifying the character set encoding format.

1.2 Restrictions and Guidelines

You can adopt UTF-8/GBK to perform configuration in Chinese. When you use the cursor to process words or delete **Backspace** in the CLI, the interface may display errors or garbled characters. You are advised to delete

all current characters and then configure a unified character set encoding format. Upon word processing or Backspace deletion, you can run the **show running-config** command to check whether the configurations are correct. (To delete a Chinese character, you must press the **Backspace** key twice in the case of GBK, but must press the **Backspace** key three times in the case of UTF-8.)

1.3 Configuration Task Summary

CLI configuration includes the following tasks: All the configuration tasks below are optional. Select the configuration tasks as required.

- Operating the Python Script
- Configuring a Command Alias
- Configuring the Privilege Level of a Command
- Configuring the Character Set Encoding Format

1.4 Operating the Python Script

1. Overview

This section describes how to load and unload the Python script of CLI.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Operate the Python script. The configuration steps below are mutually exclusive. Select one of them for configuration.

- Load the Python script.

  cli-python insmod *python-filename*

- Unload the Python script.

  cli-python rmmod *python-filename*

1.5 Configuring a Command Alias

1. Overview

You can specify any word as the alias of a command to simplify the input of the command string.

2. Restrictions and Guidelines

- The command replaced with an alias must start from the first character of the command line.
- The command replaced with an alias must be complete.
- An alias must be entered in full; otherwise, it cannot be identified.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an alias to replace the front part of a command.

alias *mode command-alias original-command*

Default aliases are available for some commands in global configuration mode or privileged EXEC mode by default.

1.6 Configuring the Privilege Level of a Command

1. Overview

This section describes how to configure the privilege level of a command.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the privilege level of a command.

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

1.7 Configuring the Character Set Encoding Format

1. Overview

This section describes how to configure a unified character set encoding format for the device.

2. Restrictions and Guidelines

- When hybrid formats exist in current running configurations of the device, you must manually delete running configurations containing the encoding format different from the target format before modifying the character set encoding format.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the character set encoding format.

language character-set { **default** | **GBK** | **UTF-8** }

By default, hybrid formats are supported.

1.8 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-8 Monitoring of the CLI

Command	Purpose
show aliases [*mode*]	Displays all command aliases or the command aliases in specific command mode.

Contents

1 Configuring ZAM 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Restrictions and Guidelines 2
1.3 Configuring ZAM 2
1.3.1 Overview 2
1.3.2 Restrictions and Guidelines 2
1.3.3 Prerequisites 2
1.3.4 Procedure 3
1.4 Monitoring 4
1.5 Configuration Examples 4
1.5.1 Configuring ZAM 4

1 Configuring ZAM

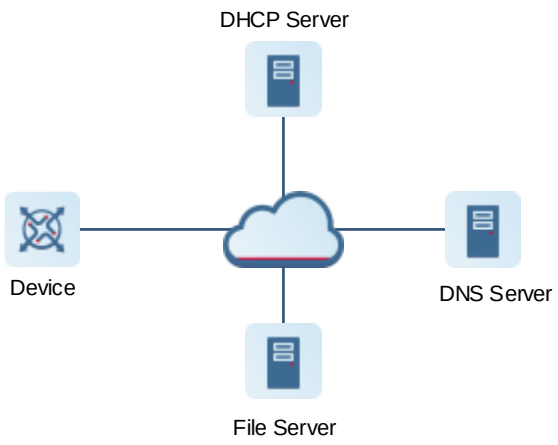
1.1 Introduction

1.1.1 Overview

The zero automatic manager (ZAM) function enables the device to automatically download the software version, upgrade the device version, and apply configuration files when the device has no configuration and the network administrator is not in contact with the field devices. ZAM simplifies the operation, maintenance, and deployment of massive devices, lowers the labor cost, reduces human errors, and improves the efficiency of network deployment.

1.1.2 Principles

Figure 1-1 ZAM Automatic Go-Online Solution



ZAM go-online and deployment include four stages as follows:

(1) Initialization

At this stage, a device that goes online without configurations connects to a network and completes initialization. The device automatically pre-deploys the ZAM environment. During the pre-deployment, the MGMT port or service port must be used as the ZAM interface. The device automatically performs configuration, without any need of extra configuration by the administrator.

(2) DHCP

Upon the pre-deployment above, the ZAM interface requests an IP address from the Dynamic Host Configuration Protocol (DHCP) server via the DHCP protocol. In a reply packet, the reply packet carries Option 66 (containing the IP address of the file server) and Option 67 (containing the name of the Python script to be downloaded). The requirements are as follows:

- The ZAM interface supports DHCP.
- Configure the ZAM interface with a DHCP-allocated IP address. DHCP requests support Option 66 and Option 67, and Option 66 and Option 67 have been configured in the address pool of the DHCP server.

- The device analyzes and deploys the IP address of the ZAM interface, and analyzes the content of Option 66 and Option 67.

(3) TFTP

According to the Python script file name and TFTP server IP address obtained at the DHCP stage, the device downloads the configuration script.

Upon downloading above, the device executes the configuration script and downloads the corresponding configuration file or version from the TFTP server.

(4) Configuration loading

After the Python script is executed, the device restarts automatically to update the device version and load the configuration file.

1.2 Restrictions and Guidelines

- An automatic retry is available after a ZAM failure. In this case, check whether the network functions properly and whether the DHCP server is correctly configured based on the ZAM failure prompt.
- For a product version with ZAM disabled by default, please manually enable this function.

1.3 Configuring ZAM

1.3.1 Overview

This section describes how to configure ZAM to enable a device with no configurations to implement automatic deployment.

1.3.2 Restrictions and Guidelines

To use the ZAM function, deploy the Trivial File Transfer Protocol (TFTP) server and DHCP server.

1.3.3 Prerequisites

- Configure the address pool, Option 66, and Option 67 for the DHCP server. The configuration example is as follows:

```
ip dhcp pool poap
 option 67 ascii zam.py
 option 66 ascii 100.1.1.2
```

- Configure the TFTP server. Store the Python script file in the root directory of the TFTP server, and create the folders listed in Table 1-1 in the root directory to store the files required during the ZAM configuration.

Table 1-1 Description of Folders to Be Created on the TFTP Server

Folder Name	Content	Function
POAP_CFG	● xxxx.cfg ● xxxx.params	● xxxx.cfg: Indicates the configuration file of the device. The configuration file of each device is named after the sn value of the device and uses .cfg as the suffix. ● xxxx.params: Indicates the parameter file of the device. It contains the path to the downloaded configuration file, path to the file used for version upgrade, and the name of the version file. ● The device automatically downloads the files.
POAP_IMAGE	Version binary file	● The folder stores the version file of the device. ● The device automatically downloads the file.
POAP_LOG	Log file	● The folder stores the log files uploaded during the ZAM configuration of the device. The log files of each device are named after the sn value of the device. ● The device automatically uploads the files.
POAP_STARTUP	Device sn value files	● The folder stores the sn value file of the device where ZAM needs to be configured. ● The device automatically uploads the file.
POAP_STATUS	-	● The folder stores the ZAM result log files, which are named after the sn value. ● The device automatically uploads the files.

1.3.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable ZAM.

zam

The ZAM function is enabled by default.

1.4 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2 ZAM Monitoring

Command	Purpose
show zam	Displays the current configurations and status of ZAM.
debug zam	Enables the ZAM framework event debugging.

1.5 Configuration Examples

1.5.1 Configuring ZAM

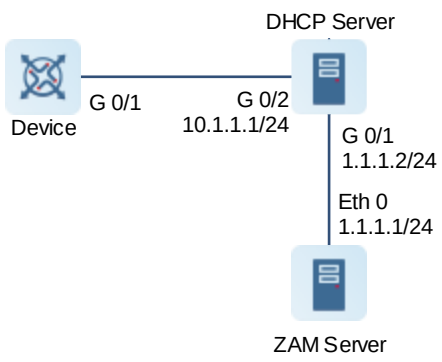
1. Requirements

dut1-standalone and dut2-VSU belong to different subnets, dut2-VSU and the ZAM server belong to the same network segment, and dut1-standalone and the ZAM server belong to different segments. ZAM needs to be configured on dut1-standalone and ut2-VSU to implement automatic upgrade and configuration delivery. The requirements are as follows:

- Configure the Secure Shell (SSH) function to allow the network management system (NMS) to manage the devices remotely via SSH. Configure a ciphertext password, with the length of no less than eight characters including letters, digits, and special characters. dut1-standalone and dut2vsu must have different usernames and passwords.

2. Topology

Figure 1-2 ZAM Topology



3. Notes

- Configure the DHCP server.
- Configure the ZAM server.
- Enable the ZAM function on the devices.

4. Procedure

(1) Configure the DHCP server.

Set the IP address of interface GigabitEthernet 0/1 of the DHCP server to 1.1.1.2/24.

```
Dhcp_Server> enable
Dhcp_Server# configure terminal
Dhcp_Server(config)#interface gigabitEthernet 0/1
Dhcp_Server(config-if-GigabitEthernet 0/1)# ip address 1.1.1.2 255.255.255.0
Dhcp_Server(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of interface GigabitEthernet 0/2 of the DHCP server to 10.1.1.1/24.

```
Dhcp_Server(config)#interface gigabitEthernet 0/2
Dhcp_Server(config-if-GigabitEthernet 0/2)# ip address 10.1.1.1 255.255.255.0
Dhcp_Server(config-if-GigabitEthernet 0/2)# exit
```

Enable the DHCP server function.

```
Dhcp_Server(config)# service dhcp
```

Configure the address pool of the DHCP server.

```
Dhcp_Server(config)# ip dhcp pool zam
Dhcp_Server(dhcp-config)# network 10.1.1.1 255.255.255.0
Dhcp_Server(dhcp-config)# default-router 10.1.1.1
```

Configure Option 66.

```
Dhcp_Server(dhcp-config)# option 66 ascii 1.1.1.1
```

Configure Option 67.

```
Dhcp_Server(dhcp-config)# option 67 ascii zam.py
```

(2) Configure the ZAM server. Store the intermediate file (Python script named **zam.py**), and the configuration files and version files to be delivered to the devices on the ZAM server. For details, see 1.3.3 Prerequisites.

(3) Enable the ZAM function on the devices.

Delete the configuration files from the devices.

```
Device# delete config.text
Do you want to delete [flash:/config.text]? [Y/N]:y
Delete success.
```

Run the **reload** command to restart the devices to enable the ZAM function.

```
Device# reload
Reload system?(Y/N)y
Device#[1042947.400971] %SYS-0-REBOOT: Rebooting by job: dp_mom_thread/3877
[1042947.408318]
```

```
U-Boot 1.4.12--g1b6cd5f (Dec 17 2019 - 21:58:43 +0800)

I2C:   ready
DRAM:  1 GiB
NAND:  512 MiB
......
......
*Apr  7 19:22:16: %DHCP_CLIENT-6-ADDRESS_ASSIGN: Interface GigabitEthernet 0/1
assigned DHCP address10.1.1.10, mask 255.255.255.0.
*Apr  7 19:22:15: %ZAM-6-EVENT: Get tftp server ip 1.1.1.1.
*Apr  7 19:22:15: %ZAM-6-EVENT: Get boot file name zam.py.
*Apr  7 19:22:21: %ZAM-6-EVENT: Download script zam.py succ.
*Apr  7 19:22:21: %ZAM-6-INFO: Begin to exec script zam.py.
......
exec cmd cd /data
mv G1M91T8000415.CFG config.text success
......
upload zam_cli.elf "exec" "copy flash:G1M91T8000415.LOG
oob_tftp://1.1.1.1/POAP_LOG/G1M91T8000415.LOG" succ
upload zam_cli.elf "exec" "copy flash:G1M91T8000415.ok
oob_tftp://1.1.1.1/POAP_STATUS/G1M91T8000415.ok" succ
*Apr  7 19:22:28: %ZAM-6-INFO: Scipt exec succ,device reset now.
Press RETURN to get started
```

5. Verification

Run the **show dhcp lease** command to display the obtained IP address.

```
Device# show dhcp lease
Temp IP addr: 0.0.0.0  for peer on Interface: Mgmt 0
Temp  sub net mask: 0.0.0.0
   DHCP Lease server: 0.0.0.0, state: 3 Init-proc
   Retry count: 7   Client-ID: 01800588aba05e4D676D7430
Temp IP addr: 10.1.1.2  for peer on Interface: VLAN 1
Temp  sub net mask: 255.255.255.0
   DHCP Lease server: 10.1.1.1, state: 9 Inform-proc
   DHCP transaction id: 75cf492b
   Lease: 86400 secs,  Renewal: 43200 secs,  Rebind: 75600 secs
   Next timer fires after: 43054 secs
   Retry count: 0   Client-ID: 01800588aba05d564C414E31
```

Run the **show zam** command to check the execution status of the ZAM function.

```
Device# show zam
ZAM state           :enable
ZAM status          :Now is waiting for dhcp wait
Server ip           :172.26.1.33
Usb path            :NULL
```

```
Interface name       :VLAN 1
Interface type       :SVI
Succ Interface name   :VLAN 1
Script URL          :NULL
```

6. Configuration Files

- DHCP server configuration file

```
hostname Dhcp_Server
!
ip dhcp pool zam
 option 66 ascii 1.1.1.2
 option 67 ascii zam.py
 network 10.1.1.0 255.255.255.0
 default-router 10.1.1.1
!
end
```

7. Common Errors

- The network connection between the device and the ZAM server is abnormal.
- The configuration file on the device is not deleted.

Contents

1 Configuring Basic Management 1
1.1 Overview 1
1.2 Basic Concepts 1
1.3 Configuration Task Summary 2
1.4 Configuring Passwords and Privilege Levels 2
1.5 Configuring Login and Authentication 4
1.5.1 Configuration Tasks 4
1.5.2 Configuring Local User Authentication and Line-based Login Authentication 5
1.5.3 Configuring Telnet Login 6
1.6 Configuring Basic System Parameters 7
1.6.1 Configuration Tasks 7
1.6.2 Configuring the System Clock 7
1.6.3 Configuring a System Name and Command Prompt 8
1.6.4 Configuring System Notifications 8
1.7 Enabling or Disabling a Specific Service 10
1.8 Rolling Back System Configurations 10
1.9 Configuring Multiple-configuration Booting 11
1.10 Configuring a Restart Policy 12
1.10.1 Configuration Tasks 12
1.10.2 Configuring Immediate Restart 12
1.10.3 Configuring Scheduled Restart 13
1.11 Running Batch File Commands 13

1.12 Configuring the Telnet Service 14

1.13 Configuring Automatic Configuration File Backup to a Remote Server 16

1.14 Monitoring 16

1.15 Configuration Examples 17

1.15.1 Configuring Login Authentication and Telnet Service 17

1.15.2 Configuring Basic System Parameters 18

1 Configuring Basic Management

1.1 Overview

Basic management refers to a series of basic network device management functions, including monitoring and maintenance. This document describes the principles, configuration methods, and configuration examples of these basic management functions.

1.2 Basic Concepts

Table 1-1 Basic Concepts

Concept	Description
TFTP	The Trivial File Transfer Protocol (TFTP) is a protocol used for simple file transfer between a client and a server in the Transmission Control Protocol (TCP)/Internet Protocol (IP) suite.
AAA	Authentication, Authorization and Accounting (AAA), including: ● Authentication: Verifies user identities and available network services. ● Authorization: Grants network services to users according to authentication results. ● Accounting: Records the network service consumption of users and to send the records to the billing system. After the AAA mode is enabled, some servers (or the local user database) are used to authenticate users' management permissions according to their usernames and password at terminal login and the configured AAA login authentication method list. For details about AAA, see "Configuring AAA" in the *Security Configuration Guide*.
RADIUS	The Remote Authentication Dial In User Service (RADIUS) is the most widely used AAA protocol.
Telnet	Telnet is a terminal emulation protocol in the TCP/IP protocol suite which provides a connection to a remote host by creating a virtual terminal. It is a standard protocol at Layer 7 (application layer) of the Open System Interconnection (OSI) model and is used on the Internet for remote login. During remote login through telnet, users must enter the usernames and passwords for authentication. Telnet sets up a connection between the local personal computer (PC) and a remote host.
System information	System information includes the system description, system power-on time, system hardware and software versions, control-layer software version, and boot-layer software version.

Concept	Description
Hardware information	Hardware information includes the physical device information as well as information about pluggable modules on the device. ● The device information includes the device description and slot quantity. ● The slot information includes the slot ID, module description (which is empty if a slot does not have a module), number of physical ports on a module inserted into a slot, and maximum number of ports supported by a slot.
System configurations	System configurations include: ● Running configurations: Configurations running on all component modules of the system. ● Startup configurations: Configurations stored in the non-volatile random-access memory (NVRAM) of the system.

1.3 Configuration Task Summary

All the following configuration tasks are optional and may be selected as needed.

- Configuring Passwords and Privilege Levels
- Configuring Login and Authentication
- Configuring Basic System Parameters
- Enabling or Disabling a Specific Service
- Rolling Back System Configurations
- Configuring Multiple-configuration Booting
- Configuring a Restart Policy
- Running Batch File Commands
- Configuring the Telnet Service
- Configuring Automatic Configuration File Backup to a Remote Server

1.4 Configuring Passwords and Privilege Levels

1. Overview

Passwords and privilege levels can be configured to control network terminals' access to network devices.

16 privilege levels from 0 to 15 are defined for users in the command line interface (CLI) of network devices. Users of various privilege levels can run different commands. A smaller value indicates a lower privilege level. Level 0 is the lowest level and users of this level can run only a few commands, whereas level 15 is the highest level and users of this level can run all commands. Levels 0 and 1 are common user levels without the device configuration permission (users are not allowed to enter the global configuration mode). Levels 2 to 15 are privileged user levels with the device configuration permission.

Password protection is configured for each privilege level on the device so that users of different levels can use different command collections. An increase in privilege level requires the input of the correct password of the target privilege level, whereas a reduction in privilege level does not require password input.

Passwords fall into two types: passwords and secrets.

- Passwords are simple encrypted passwords. You can set them for privilege levels 1 to 15.
- Secrets are secure encrypted passwords. You can set them for privilege levels 1 to 15.

Passwords must be stored in encryption mode. Passwords use simple encryption, and secrets use secure encryption.

Caution

- If a privilege level is configured with both a password and a secret, the password does not take effect.
- If no password is configured for a privileged user level, you do not need to input a password to enter this level. For security purposes, it is recommended that a password be configured for privileged user levels.

2. Restrictions and Guidelines

- When a password or secret is configured for the first time and the plaintext string is less than eight characters or contains only one type of characters, the system prompts you that it is a weak password.
- After logging in to a device, a user can run the **enable** command to raise his/her privilege level to access commands at different privilege levels. An increase in privilege level requires the input of the correct password of the target privilege level by default.
- You can specify the **level** keyword in the password configuration command to configure a password for a specific privilege level. After you set a password for a specific privilege level, the password works for the users who need to access commands of this level.
- The **enable** commands include **enable** (for role switching), **enable password**, and **enable secret**. If no role is specified, these three commands are used to set the role configured by running the **enable** command.
- **enable password**
  - This command is used to configure passwords only for level 15 and takes effect only when no secret is configured. If you use this command to configure a password for a non-15 level, the system displays a warning and the password is automatically converted into a secret.
  - If the password and secret set for level 15 are the same, the system displays a warning.
  - If you specify an encryption type but enter a plaintext password during password configuration, you cannot enter the privileged EXEC mode again.

- To enable logging for level increase or role switching, run the **login privilege log** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) (Optional) Display help information.

help

(3) Raise the privilege level.

enable { [*privilege-level*] | [**role** *role-name*] }

When the role-based access control (RBAC) function is enabled, this command can be used to switch the terminal role. If no role is specified, the system switches to role **network-admin** by default.

(4) Enter the global configuration mode.

configure terminal

(5) Configure a password.

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

Preamble spaces are allowed in front of the password but the spaces are ignored. Intermediate and trailing spaces are recognized.

(6) Configure a secret.

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

When the RBAC function is enabled and no role is specified, this command is used to set a password for role **network-admin** by default.

(7) ((Optional) Configure the role for running the **enable** commands.

enable default role *role-name*

The default role for running **enable** commands is **network-admin**.

Only when the RBAC function is enabled, this command is available.

(8) Enable level increase logging.

login privilege log

The level increase or role switching logging function is disabled by default.

(9) Configure command privilege levels.

privilege *mode* { **all** | **level** *level* | **reset** } *command-string*

(10) (Optional) Enter the line configuration mode.

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

(11) Configure a password for line-based login.

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

(12) Verify the password for line-based login.

login

The verification function of simple login passwords is disabled for the console line and enabled for the virtual terminal lines by default.

1.5 Configuring Login and Authentication

1.5.1 Configuration Tasks

Login and authentication configuration includes the following tasks:

- Configuring Local User Authentication and Line-based Login Authentication
- Configuring Telnet Login

1.5.2 Configuring Local User Authentication and Line-based Login Authentication

1. Overview

When AAA is disabled, you can configure a line password or local user authentication to control users to log in to and manage the device. When login authentication (via the **login** command) is configured for a line, only users who pass the line password verification are allowed to log in. When local user authentication (via the **login local** command) is configured for a line, the username and password entered by a user are checked against those stored in the local user database. If they are matched, the user can access the device with proper management permissions.

When AAA is enabled, some servers can be used to authenticate users' management permissions by their usernames and passwords at their login. Only authenticated users are allowed to log in. For example, a RADIUS server can authenticate usernames and passwords and control users' permissions to manage the device. Thus, instead of using locally stored password information for authentication, the device sends encrypted user information to the RADIUS server for verification. The server configures unified usernames, passwords, shared passwords, and access policies of users to manage and control user access and improve the security of user information.

Caution

After AAA is enabled, line password verification and local user authentication do not take effect.

2. Restrictions and Guidelines

- In the enabled AAA authentication mode, set line-based login for this authentication, and use the AAA authentication methods, including RADIUS authentication, local authentication, and no authentication.
- In the enabled AAA security service, to perform non-AAA authentication for a line run the **login access non-aaa** command. The configuration is valid for all terminals.
- The **username** command is used to create a local user database for authentication. The encryption type **7** needs to be specified only when encrypted passwords are copied and pasted. If the value **7** is specified as the encryption type, the entered ciphertext string must consist of an even number of characters. The login user cannot delete his/her account.
- To lock a session, enable locking on the terminal connected to a line in line configuration mode, and run the **lock** command in the EXEC mode of the terminal to lock the terminal. When a user enters any character on the locked terminal, the password prompt is displayed. The terminal will be automatically unlocked if the entered password is correct.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a local user account and optional authorization information.

username *username* [**login mode** { **console** | **ssh** | **telnet** | **ftp** }] [**online amount** *amount-number*] [**permission** *oper-mode path*] { [**privilege** *privilege-level*] | [**role** *text-string*] } [**reject remote-login**] [**web-auth**] [**pwd-modify**] [**nopassword** | **password** [**0** | **7**] *text-string* | **secret** [**0** | **5** | **8**] *text-string*]

No local user account or authorization information is configured by default.

(4) (Optional) Import user information from a file.

username import *filename*

(5) (Optional) Export user information to a file.

username export *filename*

(6) (Optional) Enter the line configuration mode.

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

(7) Configure the connection timeout time.

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

The default connection timeout time is 10 minutes.

If there is no input information during the specified time, the server interrupts the established connection.

(8) Configure the session timeout time.

session-timeout *session-timeout-time* [**output**]

The default session timeout time is 0 minute for remote terminals. That is, the sessions never time out. If there is no input information during the specified time, the device closes sessions established to a remote terminal on the current line and restores the terminal to the idle state.

(9) Configure local authentication for line-based login.

login local

When AAA is disabled, no local user authentication is configured for lines by default.

(10) (Optional) Configure non-AAA authentication for line-based login when AAA is enabled.

login access non-aaa

When AAA is enabled, non-AAA authentication is disabled by default.

(11) (Optional) Enable locking on a terminal connected to a line.

lockable

The function of locking terminals connected to the current line is disabled by default.

(12) Return to the privileged EXEC mode.

end

(13) Lock the terminal connected to the current line.

lock

1.5.3 Configuring Telnet Login

1. Overview

As an application-layer protocol in the TCP/IP protocol suite, telnet provides the standard for remote login and virtual terminal communication on the Internet. The telnet client service allows a local or remote login user of the device to access other remote system resources on the Internet.

2. Restrictions and Guidelines

If you have run the **telnet** command to initiate a telnet client session, you can press **Ctrl+Shift+6+X** (press **Ctrl+Shift+6**, release the buttons, and then press **X**) to temporarily exit the session. To restore this session, run the <**1–99**> command. To display information about established sessions, run the **show sessions** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Run the **telnet** command to log in to the telnet server.

telnet [**oob**] { *hostname* | *ipv4-address* | *ipv6-address* } [*port-number*] [**/source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** *interface-type interface-name* }] [**via** *mgmt-name*]

(3) Run the **do telnet** command to log in to the telnet server.

do telnet [**oob**] { *hostname* | *ipv4-address* | *ipv6-address* } [*port-number*] [**/source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** *interface-type interface-name* }] [**via** *mgmt-name*]

(4) (Optional) Restore the established telnet client session.

1–99

(5) (Optional) Disconnect a suspended telnet client session.

disconnect *session-id*

(6) Enter the global configuration mode.

configure terminal

(7) Enable the telnet server service.

enable service telnet-server

1.6 Configuring Basic System Parameters

1.6.1 Configuration Tasks

Basic system parameter configuration includes the following tasks:

- Configuring the System Clock
- Configuring a System Name and Command Prompt
- Configuring System Notifications

1.6.2 Configuring the System Clock

1. Overview

The system clock includes the date (year, month, and day), time (hour, minute, and second), and week information. This function is used to record event occurrence time, such as the system logging. When you use a device for the first time, set its system time to the current date and time manually.

2. Restrictions and Guidelines

- The device clock starts from the configured time and keeps running even when the device is powered off.
- If a device has no hardware clock, the manually configured time becomes invalid when the device is

powered off.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure the system date and clock.

clock set *hh:mm:ss* [*MM* [*DD* [*YY*]]]

(3) (Optional) Update the hardware clock.

clock update-calendar

(4) (Optional) Synchronize the software clock with the hardware time.

clock read-calendar

(5) (Optional) Configure the summer time.

clock summer-time *summer-time-zone* **start** *start-month* [*week* | **last**] *start-date hh:mm* **end** *end-month* [*week* | **last**] *end-date hh:mm* [**ahead** *hours-offset* [*minutes-offset*]]

(6) (Optional) Configure the time zone.

clock timezone *timezone hours-offset* [*minutes-offset*]

1.6.3 Configuring a System Name and Command Prompt

1. Overview

To facilitate management, you can configure a system name for each device to identify the device. The default system name is **Ruijie**, and acts as the default command prompt. The command prompt changes with the system name. A system name longer than 32 characters is truncated to keep only the first 32 characters.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a system name.

hostname *hostname*

The default host name is **Ruijie**.

(4) Configure a command prompt.

prompt *prompt-string*

No CLI prompt is configured by default, and the system name is used as the command prompt.

1.6.4 Configuring System Notifications

1. Overview

System notifications are prompts displayed after user login and are classified into the following two types:

- Message of the day (MOTD): Sends urgent messages to users. MOTD information is displayed on the

terminal after a user logs in to the device.

- Login banner: Provides some common login prompts and appears after MOTD information.

2. Restrictions and Guidelines

After entering a delimiter and pressing **Enter**, you can enter text, and then enter a delimiter and press **Enter** again to stop entering the text. Any characters following the ending delimiter are dropped. Text in the notification information must not contain the delimiter letter.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure MOTD information.

banner motd *c message c*

No MOTD information is configured by default.

(4) Configure login banner information.

banner login *c message c*

No login banner information is configured by default.

(5) Configure a prompt indicating the establishment of a reverse telnet connection.

banner incoming *c message c*

No prompt for the establishment of a reverse telnet connection is configured by default.

(6) Configure a prompt for the access to the privileged EXEC mode.

banner privilege-mode *c message c*

No prompt for the access to the privileged EXEC mode is configured by default.

(7) Configure a prompt for SLIP/PPP line connection.

banner slip-ppp *c message c*

No prompt for SLIP/PPP line connection is configured by default.

(8) Configure a prompt for user login authentication timeout.

banner prompt-timeout *c message c*

No prompt for user login authentication timeout is configured by default.

(9) (Optional) Enter the line configuration mode.

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

(10) Configure a welcome prompt indicating that a user has entered the user EXEC mode of a line.

banner exec *c message c*

No welcome prompt indicating that a user has entered the user EXEC mode of a line is configured by default.

(11) (Optional) Configure a prompt indicating that the function of displaying EXEC prompt information is activated again for a specific line.

banner exec-banner *c message c*

The function of displaying EXEC prompt information is activated for all lines by default.

1.7 Enabling or Disabling a Specific Service

1. Overview

When the system is running, you can dynamically adjust system services and enable or disable specific services (SSH server service, telnet server service, SNMP agent service, and Web server service).

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable a specific service.

enable service { **ssh-server** | **telnet-server** | **snmp-agent** | **web-server** }

The Simple Network Management Protocol (SNMP) agent service is enabled and the telnet server, Secure Shell (SSH) server, and Web server services are disabled by default.

(4) (Optional) Save system configurations (**running-config**) to a specific position.

write [**auto-save interval** *interval-time* | **memory** [**auto-save interval** *interval-time*] | **terminal**]

1.8 Rolling Back System Configurations

1. Overview

Rollback configuration allows you to make a snapshot for the current configurations, that is, a copy or checkpoint of the current configurations, and apply the checkpoint configurations to the device without restarting the device. This function applies to the following scenarios:

- When current system configurations contain too many errors to locate or roll back one by one, you must roll back the current configurations to a previous correct state.
- When the device application environment changes and the device needs to run the configurations in a configuration file, you can roll back the current configurations to the specified configuration file state without restarting the device.

During rollback, the system compares and handles the differences between the current configurations and checkpoint configurations.

- For the same commands in both configurations, the system does not process them.
- For the commands only in the current configurations, the system cancels them.
- For the commands only in the checkpoint configurations, the system runs them.
- For the different commands between both the current configurations and checkpoint configurations, the system cancels them, and then runs related commands in the checkpoint configurations.

2. Restrictions and Guidelines

- The checkpoint quantity is controlled using the internal function macro. For devices with a small flash memory, four checkpoints are supported. The default checkpoint quantity is **10**.
- Only one user can create checkpoints and configure rollback on a device at a time.
- It is recommended that you check the consistency of serial port baud rates between the current system configurations and checkpoint configurations before you perform rollback. If they are inconsistent, you are advised to change the serial port baud rate to that of the checkpoint configurations. Otherwise, a rate change will occur during rollback, causing a failure to display the rollback process information.
- During configuration rollback, do not hot-swap any supervisor module, line card, or service board and ensure that the device topology environment is the same as the environment of checkpoint creation. For example, if the device topology is a standalone environment during checkpoint creation but a virtual switching unit (VSU) environment during rollback, configuration rollback may fail.
- If an “Increased configuration:” message is displayed after rollback, configurations increase from the checkpoint configurations. This is because some commands cannot be reversed or fail to be reversed. For details, see the command manuals of specific functions, and manually reserve these commands.
- If a "Decreased configuration:" message is displayed after rollback, configurations decrease from the checkpoint configurations. This is because some commands fail to be executed during rollback. For details, see the command manuals of specific functions, and manually run these commands.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Create a checkpoint.

checkpoint [*checkpoint -name*] [**description** *description*]

No checkpoint is configured by default.

(3) Roll back configurations.

rollback running-config checkpoint *checkpoint -name* [**display-differences** | **ignore-results**]

(4) Clear the checkpoint data.

clear checkpoint database

1.9 Configuring Multiple-configuration Booting

1. Overview

Multiple-configuration booting allows users to modify the saving paths and names of startup configuration files of the device. This function saves configurations to an extended flash memory or an extended Universal Serial Bus (USB) flash drive of the device only. To save configurations to an extended USB flash drive, the device must support at least one USB port. If the device supports two or more USB ports, this function saves startup configurations to USB 0 only.

The startup configuration file of the device is saved in the flash memory and named **config.text** by default.

2. Restrictions and Guidelines

- The startup configuration file name can be an existing path. If the path does not exist, the **write** command fails to save the configurations. For example, if the startup configuration file name is set to **flash:/Hostname/Hostname.text** or **usb0:/Hostname/Hostname.text**, **flash:/Hostname** and **usb0:/Hostname** must exist. In master-slave mode, the paths must exist on all devices.
- To save the startup configuration file to a USB flash drive, the device must provide a USB port with a USB flash drive inserted. Otherwise, the **write** command will fail to save the configurations. In master-slave mode, all devices must have a USB flash drive inserted.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Modify the saving path and name of startup configuration file.

boot config { **flash:***filename* | **usb0:***filename* }

1.10 Configuring a Restart Policy

1.10.1 Configuration Tasks

The restart policy configuration includes the following tasks:

- Configuring Immediate Restart
- Configuring Scheduled Restart

1.10.2 Configuring Immediate Restart

1. Overview

Immediate restart applies when the device needs to be restarted immediately.

2. Restrictions and Guidelines

- A restart may interrupt services. Exercise caution.
- If the device to be restarted is being upgraded, it does not perform the restart.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure immediate device restart.

reload

1.10.3 Configuring Scheduled Restart

1. Overview

A restart policy enables the device to restart as scheduled. The following two scheduled restart functions are supported:

- Configure the system to restart after an interval. The interval is in the format of *mmm* or *hhh*:*mm*, in minutes. You can select either of the formats. You can specify an interval name to reflect the restart purpose.
- Configure the system to restart at a future time point.

2. Restrictions and Guidelines

- A restart may interrupt services. Exercise caution.
- If the device to be restarted is being upgraded, the system does not perform the restart.
- The restart time must be later than the current system time but cannot be more than 31 days later than the current system time. After you configure a restart schedule, do not change the system clock (for example, change the system time to a time after the restart time). Otherwise, the configuration may fail.
- To restart the system at a future time point, the system must support the clock function and the input time value must be a future time point. The **MM DD YY** parameter is optional. If it is not specified, the system clock time is used by default. A new restart schedule overwrites the existing one. If the system is restarted before a restart schedule takes effect, the schedule will be lost.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure scheduled device restart.

- Configure a scheduled restart schedule.

  reload at *hh*:*mm*:*ss* [*MM* [*DD* [*YY*]]]

- Configure a countdown restart schedule.

  reload in { [*hh* :] *mm*] }

  No restart function is configured by default.

(3) (Optional) Cancel the restart schedule.

reload cancel

1.11 Running Batch File Commands

1. Overview

To management system functions, it may take a long time to enter many commands on the CLI. This process is prone to errors and omissions. You can put the commands in a batch file according to configuration steps, and execute the file to complete related configurations.

2. Restrictions and Guidelines

- You can specify the name and content of the batch file on your PC and transfer the file to the flash memory of the device through TFTP. The content of the batch file simulates user input. Therefore, you must edit the

content according to the configuration sequence of the CLI commands. For some interactive commands, you must write the responses in the batch file to ensure that the commands are normally run.

- The batch file must not exceed 128 KB in size; otherwise, it will fail to be executed. You can divide a large batch file into multiple files smaller than 128 KB in size each.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Run the **execute** command to execute the batch file.

execute { [**flash:**] *filename* }

1.12 Configuring the Telnet Service

1. Overview

As an application-layer protocol in the TCP/IP protocol suite, telnet provides the standard for remote login and virtual terminal communication on the Internet.

The telnet client service allows a local or remote login user of the device to access other remote system resources on the Internet. As shown in the following figure, a user uses a PC to connect to device A by using the terminal emulation program or telnet program and then logs in to device B by running the **telnet** command to configure and manage device B.

Figure 1-1 Telnet Service

The telnet program can use an IPv4

or IPv6

address for communication. The telnet server can accept

telnet connection requests from

IPv4 and IPv6 addresses. The telnet client can send connection requests

to hosts identified

by IPv4 and IPv6 addresses.

When the telnet server service is enabled on the device, you can use the telnet client to connect to the device and configure the following functions:

- Configure an access control list (ACL) for the telnet server.
- Disable the IP address blocking function of the telnet server.
- Configure the number of authentication failures, beyond which an IP address is blocked, and the time period for counting consecutive authentication failures on the telnet server.
- Configure the -period for awakening blocked IP addresses on the telnet server.

- Clear entries about blocking and authentication failures of all or specific IP addresses.

2. Restrictions and Guidelines

- When the number of authentication failures of telnet login meets the IP address blocking conditions in the authentication failure count period, the source IP address blocking is triggered. That is, the telnet client of this source IP address is not allowed to log in to the device to prevent the device from being attacked. The telnet client can log in to the device only after the IP address awakening period expires.
- In the enabled IP address blocking function, a user logs in to the device through telnet . When the number of consecutive authentication failures reaches the configured count within the authentication failure count period, source IP address blocking is triggered. When such number does not reach the configured count or one authentication operation is successful within the authentication failure count period, the authentication failures are cleared.
- After the time for awaking a blocked source IP address comes, entries about the IP address blocking are cleared. The blocked IP address is awakened immediately and can log in to the device through the telnet client.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ACL for the telnet server.

ip telnet access-class { *acl-number* | *acl-name* }

(4) Disable the IP address blocking function of the telnet server.

ip telnet ip-block disable

The IP address blocking function of the telnet server is enabled by default.

(5) Configure the number of authentication failures, beyond which an IP address is blocked, and the -period for counting consecutive authentication failures on the telnet server.

ip telnet ip-block failed-times *failed-times* **period** *failed-period-time*

The allowed maximum number of authentication failures is 6, and the -period for counting consecutive authentication failures is 5 minutes by default.

(6) Configure the -period for awakening blocked IP addresses on the telnet server.

ip telnet ip-block reactive *reactive-period-time*

The default -period for awakening blocked IP addresses is 5 minutes.

(7) Configure the -period for awakening blocked IP addresses on the telnet server.

clear telnet ip-block { **all** | [*ipv4-address* | *ipv6-address*] }

1.13 Configuring Automatic Configuration File Backup to a Remote Server

1. Overview

By configuring the specific information and interval, you can automatically back up the configuration file of the device to the remote server.

2. Restrictions and Guidelines

- If no configuration file exists during command execution, an error is displayed.
- If the configuration file is deleted after the configuration command takes effect, the system stops backing up the configuration file to the remote server after the preset time expires.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure automatic backup of the configuration file backup to a remote server.

auto-backup configuration [**oob**] { **ftp** *server* [**port** *port-number*] **username** *username* **password** { [0] *password* | 7 *encrypted-password* } | **tftp** *server* } **interval** *interval-time* [**path** *folder*]] [**via** *mgmt_name*] [**vrf** *vrf_name*]

1.14 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-2 Monitoring

Command	Purpose
show boot config	Displays the saving path and name of startup configuration file.
show checkpoint { checkpoint-name [**all**] | **summary** }	Displays all information about a checkpoint or a summary of all checkpoints.
show clock	Displays the current system time.
show line { **console** *line-number* **| vty** *line-number* **|** *line-number* }	Displays the line configurations.
show reload	Displays system restart settings.
show running-config [**interface** *interface*]	Displays the running configurations of the device system or configurations of an interface.
show startup-config	Displays the device configurations stored in the NVRAM.

Command	Purpose
show telnet ip-block { **all** | **list** }	Displays information about blocked IP addresses and authentication failures.
show this	Displays effective system configurations in current mode.
show version	Displays system information.
show service	Displays the service status (enabled/disabled).
show hostname	Displays the host name of the device.
show debugging	Displays information about enabled debugging functions.
show sessions	Displays information about established telnet client instances.
show language character-set	Displays the current character set encoding format of the device.
show calendar	Displays the hardware time.
show cpu	Displays the CPU information.
show memory [**history** | **low-watermark** | *process-id* | *process-name* | **slot** | **sorted total**]	Displays the memory information.
show memory vsd	Displays the memory information.
show pci-bus	Displays the PCI-mounted device information.
show processes cpu [**history** [**table**] | [**5sec** | **1min** | **5min** | **15min**] [**nonzero**]]	Displays the system task information.
show processes cpu detailed { *process-id* | *process*-name }	Displays the specified task information.
show usb-bus	Displays the USB-mounted device information.

1.15 Configuration Examples

1.15.1 Configuring Login Authentication and Telnet Service

1. Requirements

- Establish a telnet session to a remote device.
- Complete login identity authentication.

2. Topology

Figure 1-2 Configuring the Telnet Service

3. Notes

- Establish a telnet session to the remote device whose IP address is 192.168.65.119.
- Establish a telnet session to the remote device whose IPv6 address is 2AAA:BBBB::CCCC.

4. Procedure

(1) Configure user and authorization information.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
Hostname(config-line)# password Guestuser
Hostname(config-line)# login
```

(2) Establish a telnet session to a remote device.

Run the **telnet** command in privileged EXEC mode, or run the **do telnet** command in privileged EXEC mode, user EXEC mode, or interface configuration mode.

```
Hostname# telnet 192.168.65.119
Trying 192.168.65.119 ... Open
User Access Verification
Password: Guestuser
Hostname# telnet 2AAA:BBBB::CCCC
Trying 2AAA:BBBB::CCCC ... Open
User Access Verification
Password:
Hostname(config)# do telnet 2AAA:BBBB::CCCC
Trying 2AAA:BBBB::CCCC ... Open
User Access Verification
Password: Guestuser
```

5. Verification

- Run the **ping** command to display the configurations. If the remote device can be pinged, the telnet service is configured.
- Verify the login identity. If the login is successful, login authentication is configured.

1.15.2 Configuring Basic System Parameters

1. Notes

- Configure the system time.

- Configure MOTD information.
- Configure login banner information.
- Set the serial port baud rate to 57,600 bps.

2. Procedure

(1) Configure the system time.

Set the system time to June 20, 2003, 10:10:12.

```
Hostname> enable
Hostname# clock set 10:10:12 6 20 2003
```

(2) Configure MOTD information.

Set the MOTD content to "Notice: system will shutdown on July 6th." with the pound key (#) as the delimiter.

```
Hostname# configure terminal
Hostname(config)# banner motd #
Enter TEXT message.  End with the character '#'.
Notice: system will shutdown on July 6th.#
Hostname(config)#
```

(3) Configure login banner information.

Set the login banner content to "Access for authorized users only. Please enter your password." with the pound key (#) as the delimiter.

```
Hostname(config)# banner login #
Enter TEXT message.  End with the character '#'.
Access for authorized users only. Please enter your password.
#
```

(4) Set the serial port baud rate to 57,600 bps.

```
Hostname# configure terminal
Hostname(config)# line console 0
Hostname(config-line)# speed 57600
Hostname(config-line)# end
```

3. Verification

- Verify the system time.

Run the **show clock** command in privileged EXEC mode to display the system time.

```
Hostname# show clock
clock: 2003-6-20 10:10:54
```

- Verify MOTD information.

Connect to the local device through the console, telnet, or SSH, and check whether the MOTD information is displayed before the CLI appears.

```
Hostname# telnet 192.168.65.236
Notice:  system will shutdown on July 6th.
Access for authorized users only. Please enter your password.
 User Access Verification
```

```
Password:
```

- Verify login banner information.

  Connect to the local device through the console, telnet, or SSH, and check whether the login banner information is displayed before the CLI appears.

```
Hostname# telnet 192.168.65.236
Notice:  system will shutdown on July 6th.
Access for authorized users only. Please enter your password.
 User Access Verification
Password:
```

- Verify that the serial port baud rate is set to 57,600 bps.

  Run the **show line** command to display the configurations.

```
Hostname# show line console 0
CON     Type    speed   Overruns
* 0     CON     57600   0
Line 0, Location: "", Type: "vt100"
Length: 25 lines, Width: 80 columns
Special Chars: Escape  Disconnect  Activation
             ^^x    none       ^M
Timeouts:     Idle EXEC    Idle Session
             never       never
History is enabled, history size is 10.
Total input: 22 bytes
Total output:  115 bytes
Data overflow:  0 bytes
stop rx interrupt:  0 times
Modem: READY
```

Contents

1 Configuring RBAC 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Basic Concepts 1
1.2 Configuration Task Summary 3
1.3 Configuring a Feature Group 3
1.3.1 Overview 3
1.3.2 Restrictions and Guidelines 3
1.3.3 Procedure 3
1.4 Configuring Role Permissions 4
1.4.1 Overview 4
1.4.2 Configuration Tasks 4
1.4.3 Enabling the RBAC Function 4
1.4.4 Configuring Roles 4
1.4.5 Configuring Rule Permissions for a Role 5
1.4.6 Configuring Description of a Role 6
1.4.7 Prohibiting a Role from Operating All Interface Resources 7
1.4.8 Allowing a Role to Operate a Specific Interface Resource 7
1.4.9 Prohibiting a Role from Operating All VLAN Resources 8
1.4.10 Allowing a Role to Operate a Specific VLAN Resource 8
1.4.11 Prohibiting a Role from Operating All VRF Resources 8
1.4.12 Allowing a Role to Operate a Specific VRF Resource 9

1.5 Monitoring 9

1.6 Configuration Examples..... 10

1.6.1 Configuring Role Permissions 10

1 Configuring RBAC

1.1 Introduction

1.1.1 Overview

Role-based access control (RBAC) associates roles with permissions. Users are assigned with appropriate roles with -permissions. The authorization structure of user-role-permission is formed to simplify permission management. Roles are defined to complete various tasks, and a device administrator can predefine all the roles and their permissions. To change a user's permission, use RBAC to change only the permission of his role. This process reduces the authorization workload and device management overhead.

1.1.2 Basic Concepts

- Feature

  Features vary with CLI commands. CLI commands with the same features constitute one feature.

- Feature group

  A feature group is composed of features. Different features are classified as needed to form one feature group. In short, a feature group is composed of several types of CLI commands.

- User

  By default, a user does not have any permissions to operate a device. Only after you specify a proper role to a user, the user has the permission of this role. There are local users and remote AAA server users. Local users are used for local authentication while remote AAA server users are used for remote AAA authentication.

- Role

  There are predefined system roles and user-defined roles. The system predefines 18 roles, including **network-admin**, **network-operator**, and **priv-*n*** (0–15). Each role is granted with specific operation permissions. Table 1-1 lists these roles and their permissions.

Table 1-1 Roles and Permissions

Role	Default Permission
network-admin	Administrator role, with all operation permissions.
network-operator	Operator role, with the following permissions: ● Permission control: ○ CLI commands: allowed to run the **ping**, **show**, **ssh**, **telnet**, **traceroute**, **ssh-session**, and **terminal** commands and the command to change the current local user password. The **show** command displays all information. ● Resource control: ○ Interfaces: allowed to operate all interfaces. ○ Virtual local area networks (VLANs): allowed to operate all VLANs.

	○ VPN routing and forwarding (VRF): allowed to operate all VRF instances.
priv-0	Level-0 role, assigned with the following permissions: ● Permission control: ○ CLI commands: allowed to run the **ping**, **ssh**, **telnet**, **traceroute**, **ssh-session**, and **enable** commands. ● Resource control: ○ Interfaces: allowed to operate all interfaces. ○ VLANs: allowed to operate all VLANs. ○ VRF: allowed to operate all VRF instances.
priv-n (1-13)	Level-1 to level-13 roles, without any permission
priv-14	Level-14 role, with the following permissions: ● Permission control: ○ CLI commands: allowed to run CLI commands other than the **more**, **upgrade**, and **debug** commands that are executable only by an administrator. ● Resource control: ○ Interfaces: allowed to operate all interfaces. ○ VLANs: allowed to operate all VLANs. ○ VRF: allowed to operate all VRF instances.
priv-15	Level-15 role, with the same all operation permissions as the role **network-admin**.

- Permission

  Permissions fall into three modes - read, write, and execute - or into two types - rule permissions and resource permissions. Rule permissions include those of command-based rules, those of feature-based rules, and those of feature group-based rules. Resource permissions include those of interface resources, those of VLAN resources, and those of VRF resources.

  Rule permissions configured for user roles are divided into the following categories:

  - Prohibit a role from running or allow a role to execute a specific command line.
  - Prohibit a role from running or allows a role to run one or several types of commands for specified or all features.
  - Prohibit a role from running or allows a role to run one or several types of commands for all features in a feature group.

  Resources permissions configured for user roles are divided into the following categories:

  - Prohibit a role from operating or allow a role to operate all or some interfaces.
  - Prohibit a role from operating or allow a role to operate all or some VLANs.
  - Prohibit a role from operating or allow a role to operate all or some VRF instances.

1.2 Configuration Task Summary

RBAC configuration includes the following tasks:

(1) (Optional) Configuring a Feature Group

(2) Configuring Role Permissions

a Enabling the RBAC Function

b Configuring Roles

c Configuring Rule Permissions for a Role

d (Optional) Configuring Description of a Role

e (Optional) Prohibiting a Role from Operating All Interface Resources

f (Optional) Allowing a Role to Operate a Specific Interface Resource

g (Optional) Prohibiting a Role from Operating All VLAN Resources

h (Optional) Allowing a Role to Operate a Specific VLAN Resource

i (Optional) Prohibiting a Role from Operating All VRF Resources

j (Optional) Allowing a Role to Operate a Specific VRF Resource

1.3 Configuring a Feature Group

1.3.1 Overview

This section describes how to create a feature group and add features to the feature group.

1.3.2 Restrictions and Guidelines

- Feature groups predefined in the system cannot be deleted or modified.
- Up to 64 feature groups can be customized.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a feature group and enter the feature group configuration mode.

role feature-group name *group-name*

The system predefines feature groups **L2** and **L3** by default. Feature group **L2** contains all commands for functions related to L2 protocols. Feature group **L3** contains all commands for functions related to L3 protocols.

(4) Add features to the feature group.

feature *feature-name*

By default, a system predefined feature group contains default features while a user-defined feature group contains no feature.

1.4 Configuring Role Permissions

1.4.1 Overview

This section describes how to create a user role and configure its operation permissions. After a user is authenticated to get a proper role, he has operation permissions.

1.4.2 Configuration Tasks

User role permission configuration includes the following tasks:

(1) Enabling the RBAC Function

(2) Configuring Roles

(3) Configuring Rule Permissions for a Role

(4) (Optional) Configuring Description of a Role

(5) (Optional) Prohibiting a Role from Operating All Interface Resources

(6) (Optional) Allowing a Role to Operate a Specific Interface Resource

(7) (Optional) Prohibiting a Role from Operating All VLAN Resources

(8) (Optional) Allowing a Role to Operate a Specific VLAN Resource

(9) (Optional) Prohibiting a Role from Operating All VRF Resources

(10) (Optional) Allowing a Role to Operate a Specific VRF Resource

1.4.3 Enabling the RBAC Function

1. Overview

This section describes how to enable the RBAC function.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the RBAC function.

role enable

The RBAC function is disabled by default.

1.4.4 Configuring Roles

1. Overview

This section describes how to customize a role.

2. Restrictions and Guidelines

- System predefined roles cannot be deleted by running the **no** command. The default permission of only the **priv**-*n* (0–13) role can be restored by running the **default** command.
- Permissions can be added to the **priv**-*n* (0–13) role only.

- Users can customize up to 64 roles and configure permissions for the roles. .

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a role and enter the role configuration mode.

role name *role-name*

By default, the system predefines 18 roles, including **network-admin**, **network-operator**, and **priv**-*n* (0–15). Each role is granted with specific operation permissions.

1.4.5 Configuring Rule Permissions for a Role

1. Overview

This section describes how to configure the rule permissions for a role.

2. Restrictions and Guidelines

- By default, system predefined roles have predefined rule permissions while user-defined roles have no rule permission.
- During rule configuration, if the specified rule number does not exist, create a rule; otherwise, modify the rule corresponding to the specified rule number. The modified rule supports newly authenticated users only.
- A user role is allowed to create multiple rules, and permissions executable by this role is a union set of these rules. If permissions defined by these rules conflict with each other, rules with larger serial numbers prevail. For example, if command A is prohibited by rule 1, and command B is prohibited by rule 2, but command A is allowed by rule 3, rule 2 and rule 3 finally take effect. Specifically, command A is allowed and command B is prohibited.
- Predefined rules for predefined roles in the system cannot be deleted or modified. If there is a conflict between system predefined rules and user-defined rules, user-defined rules prevail.
- Up to 256 rules can be configured for each role. A maximum of 1024 rules can be configured for all roles on the device.
- To configure command-based rules, follow the rules below:
  - Division of segments. To describe a multi-level mode command, divide the command character string into multiple segments by a semicolon (;). Each segment represents one or a series of commands. The command in the latter segment is used to execute the mode of a command in the preceding segment. A segment must contain at least one printable character.
  - Use of semicolons. To describe a multi-level mode command, separate the command segments with a semicolon. For example, the character string **config ; logging on** is used to grant a permission over the **logging on** command in configuration mode. The semicolon in the last command segment indicates that the permission is granted over the current mode command. For example, the character string **config ; interface *** is used to grant a permission over only the command to enter the interface configuration mode. The absence of a semicolon in the last command segment indicates that permissions are granted over the current command mode and all commands in this mode. For example,

the character string **config ; interface *** is used to grant permissions over all commands in interface mode.

- Use of asterisks. Each command segment contains at least one asterisk (*). An asterisk resides either in the middle or at both ends of a command segment. Each asterisk serves to fuzzily match a command. For example, the character string **config ; *** is used to grant permissions over all the commands in configuration mode. The character string **config ; logging * flush** is used to grant a permission over a command starting with **logging** and ending with **flush** in configuration mode. The character string **config ; logging *** is used to grant permissions over all commands starting with **logging on** in configuration mode. When an asterisk resides in the middle of a command segment and the asterisk is used to match the command, the command is matched up to only the first asterisk in the middle, and the subsequent command segments are all considered matched. An execution command must be fully matched.
- Matching of keyword prefixes. A prefix matching algorithm is used for the matching between the command keyword and the command character string. That is, if the first several consecutive characters or all characters of a keyword in the command line match the keyword defined in a rule, the command line matches this rule. Therefore, a command character string may include a partial or complete command keyword. For example, if the rule **rule 1 deny command show ssh** is effective, the **show ssh** command and the **show ssh-session** command are disabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Configure rule permissions for a role.

rule *rule-number* { **permit** | **deny** } { **command** *command-string* | { **read** | **write** | **execute** }* { **feature** [*feature-name*] | **feature-group** *feature-group-name* } }

By default, predefined roles have predefined rule permissions while user-defined roles have no rule permission.

1.4.6 Configuring Description of a Role

1. Overview

This section describes how to configure the description for a role.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Configure the description for a role.

description *description*

By default, a predefined role is provided with a default description with the user-defined role is provided with no description.

1.4.7 Prohibiting a Role from Operating All Interface Resources

1. Overview

This section describes how to prohibit a role from -creating, deleting or applying all interface resources.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all interface resources and enter the role interface configuration mode.

interface policy deny

By default, a role has the permission to operate all interface resources.

1.4.8 Allowing a Role to Operate a Specific Interface Resource

1. Overview

This section describes how to allow a role to create, delete or apply a specific interface resource.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all interface resources and enter the role interface configuration mode.

interface policy deny

(5) Enable the role to operate a specific interface resource.

permit interface *interface-type interface-number-list*

By default, a role is prohibited from operating all interface resources.

1.4.9 Prohibiting a Role from Operating All VLAN Resources

1. Overview

This section describes how to prohibit a role from creating, deleting or applying all VLAN resources.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all VLAN resources and enter the role VLAN configuration mode.

vlan policy deny

By default, a role has the permission to operate all VLAN resources.

1.4.10 Allowing a Role to Operate a Specific VLAN Resource

1. Overview

This section describes how to allow a role to create, delete, and apply a specific VLAN resource.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all VLAN resources and enter the role VLAN configuration mode.

vlan policy deny

(5) Allow a role to operate a specific VLAN resource.

permit vlan *vlan-list*

By default, a role is prohibited from operating all VLAN resources.

1.4.11 Prohibiting a Role from Operating All VRF Resources

1. Overview

This section describes how to prohibit a role from creating, deleting or applying all VRF resources.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all VRF resources and enter the role VRF configuration mode.

vrf policy deny

By default, a role has the permission to operate all VRF resources.

1.4.12 Allowing a Role to Operate a Specific VRF Resource

1. Overview

This section describes how to allow a role to create, delete or apply a specific VRF resource.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the role configuration mode.

role name *role-name*

(4) Prohibit a role from operating all VRF resources and enter the role VRF configuration mode.

vrf policy deny

(5) Enable a role to operate a specific VRF resource.

permit vrf *vrf-name*

By default, a role is prohibited from operating all VRF resources.

1.5 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** command to clear information.

Caution

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

Run the **debug** command to output various debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2 RBAC Monitoring

Command	Purpose
show role [**name** *role-name*]	Displays the information about a specific role or all roles.
show role feature [**detail** | **name** *feature-name*]	Displays the basic information or details about a specific feature or all features.
show role feature-group [**detail** | **name** *group-name* [**detail**]]	Displays the basic information or details about a specific feature group or all feature groups.
debug rbac	Debugs the RBAC module.

1.6 Configuration Examples

1.6.1 Configuring Role Permissions

1. Requirements

(1) Create the role **test**, set the description to "test role", and configure permissions to:

- Check all device information.
- Execute all commands of features snmpd and syslogd.
- Execute commands to create and delete interfaces, VLANs and VRF instances.
- Prohibit the role from operating all interface resources, but allow the role to operate interface VLAN 1.
- Prohibit the role from operating all VLAN resources, but allow the role to operate VLAN 1.
- Prohibit the role from operating all VRF resources, but allow the role to operate the VRF instance **test**.

(2) Create a user with username **user**, password **user123**, and role **test**.

(3) Configure username and password-based authentication for telnet login.

(4) Let a user log in to a device from a PC in telnet mode, and perform authentication with username **user** and password **user123**. Upon login, the user is assigned with role **test** and has permissions of role **test**.

2. Topology

Figure 1-1 Configuring Role Permissions

3. Notes

- Enable the RBAC function.
- Create a role and configure its description.
- Configure role permissions to:

- Operate all **show** commands.
- Operate all read, write, and execution commands of features snmpd and syslogd.
- Execute interface, VLAN and VRF commands, as well as all commands in corresponding modes.
- Prohibit the role from operating all interface resources, but allow it to operate interface vlan 1.
- Prohibit the role from operating all VLAN resources, but allow it to operate VLAN 1.
- Prohibit the role from operating all VRF resources, but allow it to operate VRF instance **test**.
- Create a user with username **user** and password **user123**, and assign the user with the role **test**.
- Configure username and password-based authentication for Telnet login.

4. Procedure

(1) Enable the RBAC function.

Enable the RBAC function for device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# role enable
```

(2) Create a role and configure its description.

Create the role **test** for device A and set the description for the role.

```
DeviceA(config)# role name test
DeviceA(config-role)# description test role
```

(3) Configure the role permissions.

Allow the role to run all **show** commands.

```
DeviceA(config-role)# rule 1 permit command show *
```

Allow the role to operate all read, write, and execute commands of features snmpd and syslogd.

```
DeviceA(config-role)# rule 2 permit read write execute feature snmpd
DeviceA(config-role)# rule 3 permit read write execute feature syslogd
```

Allow the role to execute interface, VLAN and VRF commands, as well as all commands in corresponding modes.

```
DeviceA(config-role)# rule 4 permit command config;interface *
DeviceA(config-role)# rule 5 permit command config;vlan *
DeviceA(config-role)# rule 6 permit command config;vrf definition *
```

Prohibit the role from operating all interface resources, but allow it to operate interface vlan 1.

```
DeviceA(config-role)# interface policy deny
DeviceA(config-role-interface)# permit interface vlan 1
DeviceA(config-role-interface)# exit
```

Prohibit the role from operating all VLAN resources, but allow it to operate VLAN 1.

```
DeviceA(config-role)# vlan policy deny
DeviceA(config-role-vlan)# permit vlan 1
DeviceA(config-role-vlan)# exit
```

Prohibit the role from operating all VRF resources, but allow it to operate the VRF instance **test**.

```
DeviceA(config-role)# vrf policy deny
DeviceA(config-role-vrf)# permit vrf test
DeviceA(config-role-vrf)# exit
DeviceA(config-role)# exit
```

Create a user with username **user** and password **user123**, and assign the user with the role **test**.

```
DeviceA(config)# username user password user123
DeviceA(config)# username user role test
```

Configure local username and password-based authentication for remote telnet login.

```
DeviceA(config)# line vty 0 4
DeviceA(config-line)# login local
```

5. Verification

View the role information.

```
DeviceA# show role name test
Role: test
  Description: test role
  Interface policy: deny
  Permit interfaces:
  VLAN1
  VLAN policy: deny
  Permit VLANs: 1
  Vrf policy: deny
  Permit vrfs: test
  ---------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ---------------------------------------------------------------------
  1      permit      command      show *
  2      permit RWX   feature      snmpd
  3      permit RWX   feature      syslogd
  4      permit      command      config;interface *
  5      permit      command      config;vlan *
  6      permit      command      config;vrf definition *
  R:Read W:Write X:Execute
```

Run any **show** command.

```
DeviceA# show privilege
Current privilege role is test
Ruijie# show users
Line           User        Host(s)            Idle      Location
---------------- ------------ -------------------- ---------- ------------------
*  1 vty 0      user        idle               00:00:00   172.30.31.16
```

Run all read, write, and execution commands of features snmpd and syslogd.

```
DeviceA# show logging
Syslog logging: enabled
  Console logging: level debugging, 46 messages logged
```

```
  Monitor logging: level debugging, 19 messages logged
  Buffer logging: level debugging, 46 messages logged
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Count log messages: disable
  Trap logging: level informational, 46 message lines logged,0 fail
Log Buffer (Total 1048576 Bytes): have written 4462
*Oct 16 07:23:17: %CLI-6-STARTUP: Cli server process startup.
*Oct 16 07:23:17: %LOCALEAP-6-PKIMANAGE: Self-Signed PKI is activated
DeviceA# show snmp
Chassis: 60FF60
0 SNMP packets input
       0 Bad SNMP version errors
       0 Unknown community name
       0 Illegal operation for community name supplied
       0 Encoding errors
       0 Number of requested variables
       0 Number of altered variables
       0 Get-request PDUs
       0 Get-next PDUs
       0 Set-request PDUs
       0 Drop PDUs
       0 UDP parse errors
0 SNMP packets output
       0 Too big errors (Maximum packet size 1472)
       0 No such name errors
       0 Bad values errors
       0 General errors
       0 Response PDUs
       0 Trap PDUs
SNMP global trap: disabled
SNMP logging: disabled
SNMP agent: enabled
SNMP v1: enabled
```

Run the interface access command. Then, a prompt for no permission appears.

```
DeviceA(config)# snmp-server community test rw
DeviceA(config)# logging server 1.1.1.1
DeviceA(config)# interface vlan 1
DeviceA(config-if-VLAN 1)# description test
DeviceA(config-if-VLAN 1)# exit
DeviceA(config)# interface gigabitethernet 0/1
% User doesn't have sufficient privilege to execute this command.
DeviceA(config)# vlan 1
```

```
DeviceA(config-vlan)# name test
DeviceA(config-vlan)# exit
DeviceA(config)# vlan 2
% User doesn't have sufficient privilege to execute this command.
DeviceA(config)# vrf definition test
DeviceA(config-vrf)# description test
DeviceA(config-vrf)# exit
DeviceA(config)# vrf definition test1
% User doesn't have sufficient privilege to execute this command.
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
username user password user123
username user role test
!
role enable
!
role name test
 description test role
 rule 1 permit command show *
 rule 2 permit read write execute feature snmpd
 rule 3 permit read write execute feature syslogd
 rule 4 permit command config;interface *
 rule 5 permit command config;vlan *
 rule 6 permit command config;vrf definition *
 interface policy deny
  permit interface VLAN 1
 vlan policy deny
  permit vlan 1
 vrf policy deny
  permit vrf test
!
line vty 0 4
 login local
```

Contents

1 Configuring Lines 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Configuration Task Summary 1
1.3 Configuring the Number of VTY Terminals 1
1.3.1 Overview 1
1.3.2 Restrictions and Guidelines 1
1.3.3 Procedure 2
1.4 Configuring Line Attributes 2
1.4.1 Overview 2
1.4.2 Restrictions and Guidelines 2
1.4.3 Procedure 3
1.5 Configuring Terminal Attributes 6
1.5.1 Overview 6
1.5.2 Procedure 6
1.6 Monitoring 8
1.7 Configuration Examples 8
1.7.1 Configuring Line Attributes 8

1 Configuring Lines

1.1 Introduction

1.1.1 Overview

There are various types of terminal lines on network devices. You can group and manage terminal lines by types. Configurations of these terminal lines are called line configurations. On network devices, terminal lines are classified into multiple types such as CTY and virtual type terminal (VTY).

1.1.2 Principles

1. Basic Concepts

- CTY

  The CTY line is a line connected to the console port. Most network devices have one console port. You can access the local system through the console port.

- VTY

  A VTY line is a virtual terminal line not connected to any hardware. It is used for telnet or Secure Shell (SSH) connection.

1.2 Configuration Task Summary

Line configuration includes the following tasks.

The following tasks are optional. Select them based on your requirements.

- (Optional)Configuring the Number of VTY Terminals
- (Optional)Configuring Line Attributes
- (Optional)Configuring Terminal Attributes

1.3 Configuring the Number of VTY Terminals

1.3.1 Overview

This section describes how to enter the line configuration mode to configure other functions.

1.3.2 Restrictions and Guidelines

- The **line vty** command allows you to enter the VTY line configuration mode and specify the number of VTY connections.
- To reduce the number of available VTY connections, run the **no line vty** *line-number* command.
- To configure the allowed maximum number of VTY connections, run the **line maximum-vty** command. If the allowed maximum number of VTY connections is set to **0**, all remote connections fail. If the allowed maximum number of VTY connections is set to a value less than the number of online remote connections, the configuration fails and a prompt appears.

Note

- Remote connections include telnet, SSH, and session connections.
- The allowed maximum number of VTY connections and the number of available VTY connections are separately managed. A remote connection is established successfully only when both conditions are met.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the line configuration mode.

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

(4) Configure the number of VTY lines. Perform either of the following operations:

- (Optional) Increase or decrease VTY connections.

  line vty *line-number*

  There are five VTY connections, numbered from 0 to 4 by default. You can increase the number of VTY connections to 36, with new ones numbered from 5 to 35.

  VTY connections numbered from 0 to 4 are default connections of the system, which cannot be deleted. Only new connections can be deleted.

- (Optional) Configure the allowed maximum number of VTY connections.

  line maximum-vty *max-number*

  The allowed maximum number of VTY connections is **36** by default.

1.4 Configuring Line Attributes

1.4.1 Overview

This section describes how to configure line attributes in line configuration mode.

1.4.2 Restrictions and Guidelines

- When the absolute timeout time set for a line expires, the device immediately disconnects the line even if a user is operating the line terminal. Before the line is disconnected, the system displays the remaining time and a prompt, indicating that the terminal will exit.
- After a user acts as a dumb terminal to connect to the device through an asynchronous serial port, the user remotely logs in to the specified host through telnet specified in the **autocommand** command or obtains the specified application-based terminal service by running the **autocommand** command.
- The asynchronous hardware of the device generates seven data bits with parity check in flow communication mode. If parity is generated, specify seven data bits per character. If no parity is generated, specify eight data bits per character. Only early devices support five or six data bits, which are seldom used.
- By running the **flowcontrol** command, you can specify the flow control mode to keep the Tx rate of one end

the same as the Rx rate of the peer end. Since terminals cannot receive data while sending data, flow control can prevent data loss. When high-speed data processing devices communicate with low-speed data processing devices (for example, a printer communicates with a network port), you also need to enable flow control to prevent data loss. Ruijie general operating system (RGOS) provides the following two flow control modes:

- Software flow control, also called soft flow control, which uses control keys for control. The default stop and start characters for software flow control are **Ctrl+S** (XOFF, ASCII value 19) and **Ctrl+Q** (XON, ASCII value 17), respectively. You can run the **stop-character** and **start-character** commands to configure them.
- Hardware flow control, also called hard flow control, which uses hardware for control.

- In telnet connection scenarios, you can run the **terminal-type** command to configure the type of terminals simulated on the terminal connected to a line as required. Upon telnet connection, one end negotiates with the other end about the terminal type based on its terminal type configuration (telnet negotiation ID: 0x18). For details, see RFC 854. You can run the **terminal-type vt100** command to restore the default terminal type.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the line configuration mode.

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

(4) Configure line attributes. The following configurations are optional. Select them based on your requirements.

- Configure the absolute timeout time for a line.

  absolute-timeout *absolute-timeout-time*

  No absolute timeout time is configured for a line by default.
- Configure the baud rate for the current line terminal.

  speed *baudrate*

  The default baud rate is **9600**.
- Configure the character for activating a null terminal session.

  activation-character *ascii-value*

  The default character for activating a terminal session is the carriage return character (ASCII value 13).
- Enable automatic command execution.

  autocommand *autocommand-command*

  Automatic command execution is disabled by default.
- Configure the prompt for refusing line-based login.

  refuse-message [*c message c*]

  No prompt is configured for refusing line-based login by default.

- Configure a privilege level for line-based login.

  privilege level *privilege-level*

  The default privilege level for line-based login is **1**.

- Enable logging on terminals.

  monitor

  Logging is disabled on terminals by default.

- Configure location description for a specific line.

  location *location*

  No location description is configured for a specific line by default.

- Configure the maximum number of lines that are displayed on a single screen for a specific line terminal.

  length *screen-length*

  The maximum number of lines that are displayed on a single screen is **24** by default.

- Configure the access to the CLI through a line.

  exce

  Accessing the CLI through lines is enabled by default.

- Configure the character for exiting a line.

  escape-character *escape-value*

  The default character for exiting a line is **Ctrl+Shift+6** (ASCII value 30).

- Configure the hotkey for disconnecting terminal connections.

  disconnect-character *ascii-value*

  The default hotkey for disconnecting terminal connections is **Ctrl+D** (ASCII value 4).

- Configure a role for a line.

  role *role-name*

  A role is configured for each line by default. The default role for serial ports, auxiliary ports, and extended serial ports is **network-admin**. The default role for other lines is **network-operator**.

Caution

Each line is configured with 1 to 64 roles. The last role cannot be deleted. If it is deleted, a failure prompt is displayed.

(5) Configure asynchronous line attributes. The following configurations are optional. Select them based on your requirements.

- Configure the number of data bits per character for asynchronous lines in flow communication mode.

  databits *bit*

  The default number of data bits per character for asynchronous lines in flow communication mode is **8**.

- Configure the CLI character encoding format for asynchronous lines.

  exec-character-bits { **7** | **8** }

The system selects a full 8-bit ASCII character set as the CLI character set by default.

To enter Chinese characters or display Chinese characters, images, or other international characters in the CLI, run the **exec-character-bits 8** command.

- Configure the flow control mode for asynchronous lines.

  flowcontrol { **hardware** | **none** | **software** }

  No flow control is configured for asynchronous lines by default.

- Configure the parity bit for asynchronous lines.

  parity { **even** | **none** | **odd** }

  When using certain hardware (such as an asynchronous serial port and console port) for communication, you usually need to configure a parity bit.

- Configure the start character for software flow control for asynchronous lines.

  start-character *ascii-value*

  The default start character for software flow control for asynchronous lines is **Ctrl+Q** (ASCII value 17).

  After software flow control is enabled for an asynchronous line, the start character indicates the start of data transmission.

- Configure the stop character for software flow control for asynchronous lines.

  stop-character *ascii-value*

  The default stop character for software flow control for asynchronous lines is **Ctrl+S** (ASCII value 19).

  After software flow control is enabled for an asynchronous line, the stop character indicates the end of data transmission.

- Configure the number of stop bits in each byte transmitted through asynchronous lines.

  stopbits { **1** | **2** }

  The default number of stop bits in each byte transmitted through asynchronous lines is **2**.

  You should configure the stop bits for communication between an asynchronous line and the connected network device (such as a conventional numb terminal and modem).

- Configure the type of terminals simulated by an asynchronous line terminal.

  terminal-type *terminal-type-string*

  The default type of terminals simulated by a line is **vt100**.

(6) (Optional) Configure an access control list (ACL) to control terminal login.

(IPv4 network)

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

(IPv6 network)

ipv6 access-class { *acl-number* | *acl-name* } { **in** | **out** }

No ACL is configured for controlling terminal login by default.

(7) (Optional) Enable command accounting for a line.

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

The command accounting function is disabled by default.

(8) (Optional) Enable user access accounting for a line.

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

The user access accounting function is disabled by default.

(9) (Optional) Enable EXEC authorization for a line.

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

The EXEC authorization function is disabled by default.

1.5 Configuring Terminal Attributes

1.5.1 Overview

You can configure temporary terminal attributes in the CLI. These configurations are invalid after the connection is disconnected.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure terminal attributes. The following configurations are optional. Select them based on your requirements.

- Configure the number of data bits per character for asynchronous lines in flow communication mode.

  terminal databits *bit*

  The default number of data bits per character for the current terminal in flow communication mode is **8**.

- Configure the character for exiting the current terminal.

  terminal escape-character *escape-value*

  The default character for exiting the current terminal is **Ctrl+Shift+6** (ASCII value 30).

- Configure the CLI character encoding format for the current terminal.

  terminal exec-character-bits { **7** | **8** }

  To enter Chinese characters or display Chinese characters, images, or other international characters in the CLI, run the **terminal exec-character-bits 8** command.

- Configure the flow control mode for the current terminal.

  terminal flowcontrol { **hardware** | **none** | **software** }

  No flow control is configured for asynchronous lines by default.

- Configure the start character for software flow control for the current terminal.

  terminal start-character *ascii-value*

  The default start character for software flow control for the current terminal is **Ctrl+Q** (ASCII value 17).

- Configure the stop character for software flow control for the current terminal.

  terminal stop-character *ascii-value*

  The default stop character for software flow control for the current terminal is **Ctrl+S** (ASCII value 19).

- Configure the number of stop bits in each byte transmitted through the current terminal.

  terminal stopbits { **1** | **2** }

  The default number of stop bits in each byte transmitted through the current terminal is **2**.

- Configure the type of terminals simulated by the current terminal.

  terminal terminal-type *terminal-type-string*

  The default terminal type is **vt100**.

- Configure the parity bit for the asynchronous line corresponding to the current terminal.

  terminal parity { **even** | **none** | **odd** }

  No parity bit is configured for the asynchronous line corresponding to the current terminal by default.

  When using certain hardware (such as an asynchronous serial port and console port) for communication, you usually need to configure a parity bit.

- Enable historical command recording for the current terminal and configure the allowed maximum number of recorded historical commands.

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

  The historical command recording function is enabled by default, and the default number of recorded historical commands is **10**.

- Configure the maximum number of lines that are displayed on a single screen on the current terminal.

  terminal length *screen-length*

  The maximum number of lines that are displayed on a single screen is **24** by default.

- Configure location description for the current terminal.

  terminal location *location*

  No location description is configured for the current terminal by default.

- Configure the baud rate for the current terminal.

  terminal speed *baudrate*

  The default baud rate is **9600**.

- Configure the maximum number of columns that are displayed in a single line on the current terminal, that is, the line width.

  terminal width *screen-width*

  The maximum number of columns that are displayed in a single line is **79** by default.

(3) Enter the global configuration mode.

configure terminal

(4) Enter the line configuration mode.

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

(5) (Optional) Configure the login authentication timeout time for the current terminal.

timeout login response *response-timeout-time*

The default authentication timeout time for line-based login is **30** seconds.

(6) (Optional) Configure communication protocols supported by the current terminal.

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

All communication protocols are supported by default. That is, both SSH and telnet are supported.

(7) (Optional) Configure the prompt for terminal logout.

vacant-message [*c message c*]

No prompt is configured for terminal logout by default.

(8) (Optional) Configure the maximum number of columns that are displayed in a single line on the current terminal, that is, the line width.

width *screen-width*

The maximum number of columns that are displayed in a single line is **79** by default.

1.6 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear line { **console** *console-line-number* | **vty** *vty-line-number* | *line-number* }	Clears the connection status of a line.
show line { **console** *console-line-number* | **vty** *vty-line-number* | *line-number* }	Displays the line configurations.
show history	Displays historical command records of a line.
show history	Displays all historical command records.
show privilege	Display the privilege level of a line.
show user [**all**]	Displays login user information of a line.

1.7 Configuration Examples

1.7.1 Configuring Line Attributes

1. Requirements

When users use VTY connections to remotely log in to the device through telnet, the network administrator can configure VTY line attributes based on the use and security requirements of the device. Configure an ACL to control terminal login, set the privilege level of VTY line users to **14**, and require users of VTY line-based login to enter a password. Set the absolute timeout time of VTY connections to 30 minutes.

2. Topology

Figure 1-1 Configuring Line Attributes

3. Notes

- Set the maximum number of VTY line users to **6**.
- Configure an ACL to allow users of some IP addresses to access the device.
- Configure attributes of VTY line user.
- Configure the privilege level, login verification method, and verification password of VTY line users.

4. Procedure

Configure an ACL named **acl1** to control terminal login.

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit 192.168.1.0 0.0.0.255
Device(config-std-nacl)# exit
Device(config)# line v 0 6
Device(config-line)# access-class acl1 in
```

Set the maximum number of VTY line users to **6**.

```
Device(config)# line v 0 6
```

Set the baud rate to 115200 bps.

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

Set the number of data bits to **8**.

```
Device(config-line)# databits 8
```

Set the parity bit to **even**.

```
Device(config-line)# parity even
```

Set the number of stop bits to **1**.

```
Device(config-line)# stopbits 1
```

Set the absolute timeout time of VTY connections to 30 minutes.

```
Device(config-line)# absolute-timeout 30
```

Configure software flow control.

```
Device(config-line)# flowcontrol software
```

Set the maximum number of lines that are displayed on a single screen to **100**.

```
Device(config-line)# length 100
```

Set the maximum number of columns that are displayed in a line to **256**.

```
Device(config-line)# width 256
```

Enable historical command recording and set the number of recorded historical commands to **200**.

```
Device(config-line)# history size 200
```

Set the privilege level of line-based login to **14**.

```
Device(config-line)# privilege level 14
```

Configure the user verification method.

```
Device(config-line)# login local
Device(config-line)# exit
```

Configure a username.

```
Device(config)# username Device privilege 15 password test_1234
```

5. Verification

Users of the IP address 192.168.1.100 can log in to the device through tenet. Users beyond the IP addresses in the 192.168.1.0/24 network segment cannot log in to the device. Run the **show users** command to display users who log in to the device.

```
Device# show users
Line           User        Host(s)            Idle      Location
---------------- ------------ -------------------- ---------- ------------------
*  0 con 0      ---         idle               00:00:00   ---
   1 vty 0      Device      idle               00:00:04   192.168.1.100
```

Run the **show line vty** command to display the line status of the console.

```
Device# show line vty 1

VTY    Type    speed   Overruns
  1    VTY    115200  0
Line 2, Location: "", Type: "vt100"
Length: 100 lines, Width: 256 columns
Special Chars: Escape  Disconnect  Activation
            ^^x    ^D        ^M
Timeouts:     Idle EXEC   Idle Session
            00:10:00    never
History is enabled, history size is 200.
Total input: 0 bytes
Total output: 0 bytes
Data overflow: 0 bytes
stop rx interrupt: 0 times
```

6. Configuration Files

Device configuration file

```
hostname Device
!
username Device privilege 15 password test_1234
!
```

```
line console 0
 exec-timeout 0 0
 speed 115200
line console 0
 exec-timeout 0 0
 speed 115200
line vty 0 6
 absolute-timeout 30
 access-class acl1 in
 privilege level 14
 login local
 password test_123
 flowcontrol software
 parity even
 stopbits 1
 width 256
 length 100
 monitor
 history size 200
 speed 115200
line vty 7 35
 access-class acl1 in
 login
!
end
```

Contents

1 Configuring File System Management 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Basic Concepts 1
1.1.3 Way to Manage Files 2
1.2 Configuration Task Summary 2
1.3 Configuring a Directory 3
1.3.1 Displaying the Working Directory 3
1.3.2 Changing the Working Directory 3
1.3.3 Displaying Directory Information 3
1.3.4 Creating a Directory 3
1.3.5 Deleting a Directory 4
1.4 Configuring a File 4
1.4.1 Displaying File Content 4
1.4.2 Displaying File Information 4
1.4.3 Copying a File 4
1.4.4 Renaming a File 5
1.4.5 Deleting a File 5
1.4.6 Ejecting a USB Device 5
1.4.7 Erasing a File System 5
1.4.8 Configuring Prompt Level 6
1.5 Monitoring 6

1.6 Configuration Examples.....6

1.6.1 Configuring Basic Features of File System Management.....6

1 Configuring File System Management

1.1 Introduction

1.1.1 Overview

Files required for running a device, including configuration files and system software, are saved in the storage media of the device. File system management refers to the management of directories and files in storage media, including creation, deletion, modification and viewing of files.

1.1.2 Basic Concepts

The storage media supported by devices include fixed media (Flash) and pluggable media (USB flash drive). Each storage medium is called a file system.

1. Storage media and file system name

- The file system of Flash-type storage media is named as "flash:".
- The file system of USB drive-type storage media is named as "usb:".

2. Default file system

The file system used by default after a user logs in to the device when multiple storage media are available for the device.

3. Name of folder and file

The name of a folder or file can contain numbers, letters or special characters except asterisk (*), vertical bar symbol (|), backslash (\), slash (/), question mark (?), angle brackets (<>), quotation mark ("), and colon (:).

4. Root directory

The root directory is the default directory once the user logs in to the device. It is expressed by a slash (/). For example, "flash:/" indicates the root directory of Flash.

5. Working directory

The working directory is also called the current working directory. The default working directory is the root directory of Flash.

6. Path

The location of a file or folder.

Note

filesystem: specifies the uniform resource locator (URL) of a file system, followed by a colon (:). File systems include **flash:**, **usb:,** and **tmp:**. In addition, *directory* indicates a file name with the path, or specifies a path name. If the name starts with a slash (/), the path is an absolute path; otherwise, the path is a relative path.

1.1.3 Way to Manage Files

To manage files, log in to the system directly or use File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP).

Table 1-1 Way to Manage Files

Way to Manage Files	Application Scenario
Direct login to the system	A device fails to access information, and you need to repair the device or manage the files and directories in the device.
FTP	FTP is applicable to file transfer scenarios which do not require high security of network, and widely used for version upgrade.
TFTP	In laboratory LAN with good network conditions, use TFTP to load and upgrade versions online.

1.2 Configuration Task Summary

Configuration of file system management includes the following tasks: All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Directory
  - Displaying the Working Directory
  - Changing the Working Directory
  - Displaying Directory Information
  - Creating a Directory
- Configuring a File
  - Displaying File Content
  - Displaying File Information
  - Copying a File
  - copy source-url dstination-url
  - Renaming a File
  - Deleting a File
  - Ejecting a USB Device
  - Erasing a File System
  - Configuring Prompt Level

1.3 Configuring a Directory

1.3.1 Displaying the Working Directory

1. Overview

This feature displays the complete path of the current working directory.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Display the complete path of the current working directory.

pwd

1.3.2 Changing the Working Directory

1. Overview

This feature changes the current working directory.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Change the current working directory.

cd [*filesystem*:] [*directory*]

1.3.3 Displaying Directory Information

1. Overview

This feature displays the list of files and sub-directories under a directory.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Display the files under a directory.

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

1.3.4 Creating a Directory

1. Overview

This feature creates a directory.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Create a directory.

mkdir [*filesystem*:] *directory*

1.3.5 Deleting a Directory

1. Overview

This feature deletes a directory.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Delete an empty directory.

rmdir [*filesystem*:] *directory*

1.4 Configuring a File

1.4.1 Displaying File Content

1. Overview

This feature displays the content of a file.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Display the content of a file.

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

1.4.2 Displaying File Information

1. Overview

This feature displays the information of a file.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Display the information of a file.

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

1.4.3 Copying a File

1. Overview

This feature copies a file.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Copy a file.

copy *source-url dstination-url*

1.4.4 Renaming a File

1. Overview

This feature renames a file.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Rename a file or folder.

rename *source-url destination-url*

1.4.5 Deleting a File

1. Overview

This feature deletes a file.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Delete a file.

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

1.4.6 Ejecting a USB Device

1. Overview

This feature ejects a USB device.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Eject a USB device.

eject usb0

1.4.7 Erasing a File System

1. Overview

This feature erases a file system of a device.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Erase the file system of a USB device.

erase usb0

1.4.8 Configuring Prompt Level

1. Overview

This feature configures the prompt level for executing a file or folder.

- When the prompt level is set to **noisy**, the system asks you to confirm all the files.
- When the prompt level is set to **quiet**, the system seldom gives a prompt.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure the prompt level for operating a file.

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

1.5 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-2 File System Management Monitoring

Command	Purpose
show disk [**usb** | **flash**]	Displays the USB flash drive or Flash information.
show file systems	Displays information about file systems.
show mount	Displays information about the file system mounted on the device.

1.6 Configuration Examples

1.6.1 Configuring Basic Features of File System Management

1. Requirements

Operate the files in the device after logging in to the device through the Console port or with a Telnet connection.

2. Notes

- Display the files and sub-directories under the current directory.
- Create the **test** directory.
- Copy the **config.text** file to the **test** directory and name it **test.text**.

3. Procedure

(1) Display the files and sub-directories under the current directory.

```
Device# dir flash:/
Directory of flash:/
Number  Properties    Size           Time                  Name
------  ----------  ----------  ------------------------  --------------------
1      -rw-     9.9k       Fri Jan  3 02:49:39 2020  Hostname.text
2      -rw-     113.3M     Sat Jun 13 14:15:17 2020
3      -rw-     5.3k       Wed Jun 10 14:12:45 2020  cfgmpls
4      drwx     4.0k       Mon Jan  6 21:12:20 2020  startup
5      -rw-     2.6k       Sat Jun 13 16:13:12 2020  cfgpol
6      -rwx     1.6k       Thu May 21 13:39:30 2020  rsa1_private.bin
7      drwx     4.0k       Thu Nov 14 23:34:40 2019  vsd
8      -rw-     3.9k       Thu Jan  1 10:53:27 1970  virtual_switch.text
9      drwx     4.0k       Mon Jan  6 21:13:23 2020  uft
10      drwx     4.0k       Fri Nov 15 00:31:04 2019  rg_licns
11      -rw-     7.5k       Wed Jun 30 10:33:50 2021  config.text
…
33 files, 22 directories
1,939,972,096 bytes data total (383,688,704 bytes free)
3,959,422,976 bytes flash total (383,688,704 bytes free)
```

(2) Create the **test** directory. Copy the **config.text** file to the **test** directory and name it **test.text**.

```
Device# mkdir test
```

(3) Copy the **config.text** file to the **test** directory and name it **test.text**.

```
Device# copy config.text flash:/test/test.text
Copying, press Ctrl+C to quit
!
Accessing flash:/config.text finished, 7652 bytes prepared
Flushing data to flash:/test/test.text...
Flush data done
Copy success.
```

4. Verification

Enter the **test** directory.

```
Device# cd test
```

Display the current working path.

```
Device# pwd
flash:/test
```

Display the files under the **test** directory.

```
Device# dir
Directory of flash:/test
Number  Properties    Size           Time                  Name
```

```
------  ----------  ----------  ------------------------  --------------------
  1      -rw-     7.5k       Tue Jan  7 19:56:44 2020  test.text
1 file, 0 directories
1,939,972,096 bytes data total (383,676,416 bytes free)
3,959,422,976 bytes flash total (383,676,416 bytes free)
```

Contents

2 Configuring USB.....1

1.1 Introduction 1

1.1.1 Overview 1

1.2 Configuration Task Summary 1

1.3 Using a USB Device 1

1.4 Ejecting a USB Device.....2

1.5 Monitoring 2

1.6 Configuration Examples.....3

1.6.1 Configuring USB Basic Features.....3

1 Configuring USB

1.1 Introduction

1.1.1 Overview

Universal Serial Bus (USB) is an external bus standard. In this document, it refers to peripheral devices in line with the USB standard, such as USB flash drives. USB devices are hot-swappable. They serve to copy files (such as configuration files and log files) from a communication device or copy external data (such as system upgrade files) to an internal storage device.

USB devices are applied in scenarios such as file system management and upgrade. The detailed scenarios are specified in configuration guides for different features. This document describes only the identification, viewing, use, and removal of USB devices.

1.2 Configuration Task Summary

USB configuration includes the following tasks:

(1) Using a USB

(2) Ejecting a USB Device

1.3 Using a USB Device

1. Overview

When you insert a USB device into a USB port, the system automatically finds the USB device. The driver module of the system, upon identifying the USB device, initializes the device and loads the file system in it. Then, the system reads and writes the USB device. Run commands (**cd**, **copy, delete** or **dir**) of the file system to operate the USB device.

2. Restrictions and Guidelines

- The system only uses products that support standard Small Computer System Interface (SCSI) commands (generally USB flash drives). Other products, including USB flash drives attached to USB network interface cards (NICs) and those with virtual USB drives, are not supported.
- A USB device supports file allocation tables (FATs) only. Other file systems can be used on a USB device only after they are converted to FATs through a PC.

3. Prerequisites

Insert a USB device.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Run commands of the file system to operate the USB device. Configure one of the following tasks.

- Enter the USB device partition.

  cd usb: [*directory*]

  The path name, if not specified, is the name of the root path of the USB device partition by default.

- Copy files between file systems.

  copy *source-url dstination-url*

  When the file to be copied exists on the target URL, the target file system determines the action, for example, reporting an error, overwriting the file, or asking users to make the choice.

- Delete a file in the USB device.

  delete usb: [*file-url*]

- Check whether the file is in the USB device.

  dir usb: [*file-url*]

  The path name, if not specified, is the name of the root path of the USB device partition by default.

Note

- When multiple partitions exist in the USB device, only the first FAT partition is accessible.
- The concept of parent directory is not available for the USB device path. After accessing the USB device by running **cd usb*:**, return to the flash file system by running **cd flash:**.

1.4 Ejecting a USB Device

1. Overview

This feature ejects a USB device while keeping the data stored in the device intact.

2. Restrictions and Guidelines

- Do not remove a USB device when the system is using it. Otherwise, the data stored in the device will be damaged. Therefore, disconnect the USB device from the system before removing it.
- Upon successful disconnection, the system prints a prompt. After that, remove the device. USB device disconnection failure indicates that the system is using the device. Remove the device when the system is not using it.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Remove the USB device.

usb remove *device-id*

1.5 Monitoring

Run the **show** command to check the USB device.

Table 1-1 Monitoring

Command	Purpose
show usb	Displays the information about the inserted USB device.

1.6 Configuration Examples

1.6.1 Configuring USB Basic Features

1. Requirements

Operate the files in the device as follows after logging in to the device through the Console port or with a Telnet connection.

- Insert the USB flash drive into the port.
- Copy the **config.txt** file in the drive to **Flash**.
- Run the **usb remove** command to remove the USB device.

2. Notes

- After you insert a USB flash drive into the port, the system displays a prompt of successful loading of the drive.
- Before removing the USB device, run the corresponding command to eject it. This is to avoid an error resulted from the system using the device.

3. Procedure

(1) After you insert a USB flash drive into the port, the system finds the USB device and loads the drive. After that, the system prints the following prompt information:

```
*Jan  1 00:09:42: %USB-5-USB_DISK_FOUND: USB Disk <Mass Storage> has been inserted
to USB port 0!
*Jan  1 00:09:42: %USB-5-USB_DISK_PARTITION_MOUNT: Mount usb0 (type:FAT32),size :
15789711360B(15789.7MB)
```

Note

Mass Storage specifies the name of the identified device. “**usb0**” specifies the first USB device. **Size** specifies the size of the partition. As shown above, the USB flash drive has a space of 15789.7 MB.

(2) Copy the **config.txt** file in the drive to Flash.

```
Hostname# dir usb0:/
Directory of usb0:/
   1 -rwx           4  Tue Jan  1 00:00:00 1980  fac_test
   2 -rwx           1  Mon Sep 30 13:15:48 2013  config.txt
2 files, 0 directories
15,789,711,360 bytes total (15,789,686,784 bytes free)
Hostname#
```

```
Hostname# copy usb0:/config.txt flash:/
Copying: !
Accessing usb0:/config.txt finished, 1 bytes prepared
Flushing data to flash:/config.txt...
Flush data done
```

(3) Remove the USB device.

```
Hostnam# usb remove 0
OK, now you can pull out the device 0.
```

4. Verification

Insert the USB flash drive to check the USB device.

```
Hostname> enable
Hostname# show usb
Device: Mass Storage
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:vfat)
Size:15789711360B(15789.7MB)
Available size:15789686784B(15789.6MB)
```

Run the **dir** command to check whether the **config.txt** file in the flash is copied successfully.

```
Hostname# dir flash:/
Directory of flash:/
  20 ----           1  Thu Jan  1 00:04:51 2020  config.txt
1 files, 0 directories
5,095,424 bytes total (4,960,256 bytes free)
```

Run the **show usb** command to check whether the USB device is removed. The device with ID 0 is not displayed when the **show usb** command is run.

```
Hostname# show usb
  No partition found.
```

5. Common Errors

- A device that uses non-standard SCSI is inserted into the USB port.
- The system cannot identify the USB device as the device is not a FAT.

Contents

1 Configuring the HTTP Service 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 3
1.2 Configuration Task Summary 3
1.3 Configuring Basic Features 3
1.3.1 Overview 3
1.3.2 Configuration Tasks 3
1.3.3 Configuring HTTP Service 3
1.3.4 Configuring HTTP Redirection to HTTPS 4
1.3.5 Configuring an HTTPS Service Certificate 5
1.4 Configuring Remote HTTP Upgrade 6
1.4.1 Overview 6
1.4.2 Restrictions and Guidelines 6
1.5 Monitoring 7
1.6 Configuration Examples 7
1.6.1 Configuring Basic Features of HTTP Service 7
1.6.2 Configuring Remote HTTP Upgrade 10

1 Configuring the HTTP Service

1.1 Introduction

1.1.1 Overview

The Hypertext Transfer Protocol (HTTP) is used to transmit Web page information on the Internet. It is at the application layer of the TCP/IP protocol stack. The transport layer adopts the connection-oriented Transmission Control Protocol (TCP).

The Hypertext Transfer Protocol Secure (HTTPS) is an HTTP protocol supporting the Secure Sockets Layer (SSL) protocol. HTTPS is used to create a secure channel on an insecure network, to prevent information from being monitored and protect against man-in-the-middle attacks. HTTPS is widely used in secure and sensitive communication on the Internet, for example, electronic transaction payments.

1.1.2 Principles

1. HTTP Service

HTTP is a service provided for Web management. Users log in to devices through Web pages to configure and manage the devices.

Web management covers Web clients and Web servers. Similarly, the HTTP service adopts the client/server mode. The HTTP client is embedded in the Web browser of the Web management client. It sends HTTP packets and receives and processes HTTP response packets. The Web server (HTTP server) is embedded in devices. The information exchange between the client and the server is as follows:

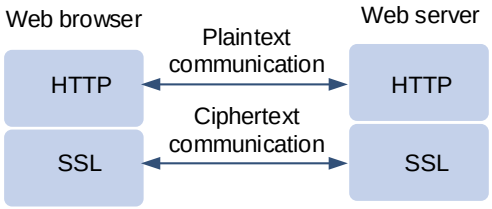
- A TCP connection is established between the client and the server. The default port number of the HTTP service is 80 and the default port number of the HTTPS service is 443.
- A TCP connection is established between the client and the server. The default port number of the HTTP service is 80 and the default port number of the HTTPS service is 4430.
- The client sends a request to the server.
- The server parses the request sent by the client. The request content includes obtaining a Web page, running a CLI command, and uploading a file.
- After executing the request content, the server sends a response to the client.
- The TCP connection between the server and the client is closed.

2. HTTPS Service

The HTTPS service is an SSL-based HTTP service, as shown in Figure 1-1. The HTTPS service improves the device security through the following services provided by the SSL protocol:

- Mutual authentication is needed between the client and the server to ensure that data is sent to the correct client and server, and unauthorized users are prevented from attacking the device.
- The communication data between the client and the server is encrypted to prevent the data from being stolen midway, ensuring security and integrity of the data transmission and achieving security management of the device.

Figure 1-1 Principle of HTTPS Service



Caution

To run HTTPS properly, a server must have a Public Key Infrastructure (PKI) certificate while a client may not.

3. HTTPS Service Certificate

An HTTPS Service certificate is used to authenticate a server and encrypt data transmission. Users can enable the device to generate a new self-signed certificate or install a trust certificate issued by the certificate authority. If the HTTPS service certificate is not trusted by the browser, the browser displays a security prompt, asking for user's confirmation before the user accesses the Web management system of the device through HTTPS. Principles are as follows:

(1) The device generates a self-signed certificate as the HTTPS service certificate upon its first startup. Users can enable the device to generate a new self-signed certificate again or install a trust certificate issued by the certificate authority.

(2) The server delivers the certificate to the browser after the browser connects to the server via HTTPS.

(3) The browser checks the certificate delivered by the server to see whether the certificate user matches the address accessed, whether the certificate is in the validity period, and whether the certificate issuer is trusted by the browser. If not, the browser displays a security prompt, asking for user's confirmation before the user accesses the server.

4. HTTP Redirection to HTTPS

HTTP redirection to HTTPS means that the device redirects the browser access request to HTTPS when a user accesses the Web management service through the HTTP. Principles are as follows:

(1) A user enters the URL of HTTP into the address bar of the browser, for example, http://192.168.1.1. The browser sends an HTTP access request to the device.

(2) The device returns an HTTP access response packet containing a redirection URL, for example, https://192.168.1.1.

(3) The browser sends an HTTPS access request to the device to access the Web management page.

5. Remote HTTP Upgrade

The device is connected to a remote HTTP server as a client and upgrades local files by obtaining files from the server. Principles are as follows:

a Connect the device to the server. Connect to the server address configured by users first.

b The device sends the version numbers of its service modules to the server.

c The server parses the version numbers and provides a file download list.

d Based on the file download list, the device connects to the file server and downloads the upgrade file. The device can connect to different servers to download different upgrade files.

e The device upgrades itself by using the upgrade file.

1.1.3 Protocols and Standards

- RFC1945: Hypertext Transfer Protocol -- HTTP/1.0
- RFC2616: Hypertext Transfer Protocol -- HTTP/1.1
- RFC2818: Hypertext Transfer Protocol Over TLS -- HTTPS

1.2 Configuration Task Summary

HTTP service configuration includes the following tasks:

(1) Configuring Basic Features

- Configuring HTTP Service
- (Optional) Configuring HTTP Redirection to HTTPS
- (Optional) Configuring an HTTPS Service Certificate

(2) Configuring Remote HTTP Upgrade

1.3 Configuring Basic Features

1.3.1 Overview

After the HTTP service is enabled on a device, users can log in to the Web management page after they pass authentication, and can monitor the device status, configure the device, upload and download files.

1.3.2 Configuration Tasks

The basic HTTP service includes the following tasks:

- Configuring HTTP Service
- (Optional) Configuring HTTP Redirection to HTTPS
- (Optional) Configuring an HTTPS Service Certificate

1.3.3 Configuring HTTP Service

1. Overview

After the HTTP service is enabled on a device, users can log in to the Web management page to manage the device after they pass authentication, and can monitor the device status, configure the device, upload and download files.

2. Restrictions and Guidelines

- Usernames and passwords involve three permission levels: Up to 10 usernames and passwords are configured for each permission level.
- By default, the system creates the account **admin**. The account cannot be deleted and only the password of

the account can be changed. The administrator account **admin** corresponds to the level 0 privilege. Account **admin** owns all function privileges on the Web client and can edit other management accounts and authorize the accounts to access pages. All new accounts correspond to the level 1 privilege.

- To change an HTTPS service port, configure the HTTPS service port.
- Users can configure an HTTPS service port number to reduce attacks initiated by unauthorized users on HTTPS service.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the HTTP service.

enable service web-server [**http** | **https** | **all**]

The HTTP and HTTPS service features are disabled by default.

(4) Configure the HTTP authentication information.

webmaster level *privilege-level* **username** *username* { **password** [**0** | **7**] *password* | **secret** [**0** | **8**] *secret* }

The permission level bound to a user is 0, username is **admin**, and plaintext password is **admin** by default.

(5) Configures an HTTP service port.

http port *port-number*

The default port number of the HTTP service is 80.

(6) Configures an HTTPS service port.

http secure-port *port-number*

The default port number of the HTTPS service is 443.

1.3.4 Configuring HTTP Redirection to HTTPS

1. Overview

After HTTP and HTTPS are enabled in the device, HTTP can automatically redirect to HTTPS to improve security when users access the Web management page of the device through HTTP.

2. Restrictions and Guidelines

- Only after the HTTP and HTTPS services are enabled, HTTP automatically redirects to HTTPS.
- If an IP address to be accessed is a Network Address and Port Translation (NAPT) address, the redirection function may fail. To access the device through HTTP, disable the NAPT feature; to access the device through HTTPS, use HTTPS directly.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure HTTP redirection to HTTPS.

web-server http redirect-to-https

Automatic HTTP redirection to HTTPS is disabled by default.

1.3.5 Configuring an HTTPS Service Certificate

1. Overview

Ruijie devices use an automatically generated self-signed certificate as the HTTPS service certificate by default. By configuring an HTTPS service certificate, the device generates a self-signed certificate again or uses the certificate assigned by Certificate Authority.

2. Restrictions and Guidelines

- The **web-server https generate self-signed-certificate** command is an interactive command. After running this command, enter the information to generate a self-signed certificate as prompted, or press **Ctrl+C** to cancel the operation.
- If the device is installed with a third-party HTTPS service certificate is installed, it uses the HTTPS certificate preferentially. The re-generated self-signed certificate does not replace the current HTTPS service certificate.
- After the HTTPS service certificate is generated again, the browser may require you to add the trust certificate again before you continue access to the Web management page of the device. You are advised to open the Web management page again after closing the browser.
- After the HTTPS service certificate is installed, the browser may require you to add the trust certificate again before you continue access to the Web management page of the device. You are advised to open the Web management page again after closing the browser.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the device to generate an HTTPS self-signed certificate again.

web-server https generate self-signed-certificate

The HTTPS service uses the self-signed certificate by default.

This command is not displayed in the configuration.

(4) (Optional) Install the HTTPS certificate.

web-server https certificate { **pem** *cert-filename* **private-key** *key-filename* } | { **pfx** *cert-filename* } [**password** *password-text*]

No HTTPS service certificate is installed by default.

This command is not displayed when the **show running-config** command is run.

1.4 Configuring Remote HTTP Upgrade

1.4.1 Overview

The device is connected to a remote HTTP server as a client and upgrades local files by obtaining files from the server.

1.4.2 Restrictions and Guidelines

- Before configuring the domain name of an HTTP upgrade server, enable the Domain Name System (DNS) on the device and configure the DNS server address.
- The server address does not support IPv6.
- Run the **http update server** command to configure the server address and port number for HTTP upgrade.
- During an HTTP upgrade, the device first connects to the server address configured by this command. If the server address is not connected, the device attempts to connect to server addresses recorded in the local file in turn. If none of the servers are connected, the upgrade cannot be performed.
- The system records the address or addresses of one or more upgrade servers. These addresses cannot be modified.
- If there is no special requirement, the HTTP upgrade time does not need to be configured by default.
- The **http update time** command can be used to change the automatic upgrade time, but can only configure a time point in each day. The time is accurate to minutes.
- In automatic upgrade mode, the device checks the file versions on the server as scheduled every day and upgrades itself by using the upgrade file.

1. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the HTTP upgrade server.

http update server { *host-name* | *ip-address* } [**port** *port-number*]

The default server address for HTTP upgrade is 0.0.0.0 and the default port number is 80.

(4) (Optional) Configure the HTTP upgrade mode.

http update mode manual

The default HTTP upgrade mode is automatic upgrade.

(5) (Optional) Configure the HTTP automatic detection time.

http update time daily *hh*:*mm*

The automatic detection time is random in the range from 00:00 to 23:59 by default.

(6) (Optional) Configure upgrade using the MGMT port.

http update set oob

The upgrade using a common port instead of a MGMT port is configured by default.

(7) Exit to the privileged EXEC mode.

end

(8) (Optional) Configure the device to detect upgrade files on the HTTP server.

http check-version [**extend**]

The function of detecting the version information of upgrade files on an HTTP server is enabled by default.

(9) Use the upgrade file to manually upgrade the specified service module.

http update { **all** | *string* }

No file for manual upgrade is configured by default.

1.5 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 HTTP Service Monitoring

Command	Purpose
show web-server status	Displays the configuration and status of the Web service.
show web-server https certificate information	Displays the HTTPS certificate of the Web server.

1.6 Configuration Examples

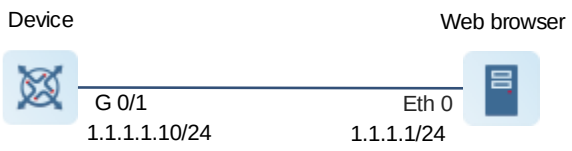
1.6.1 Configuring Basic Features of HTTP Service

1. Requirements

To manage a Ruijie device in Web mode, log in to the device through a Web browser and configure related features.

2. Topology

Figure 1-2 Topology for Basic Features of HTTP Service



3. Notes

- Configure L3 route reachable between the server and the device.
- To improve security, change the authentication username, HTTP service port, and HTTPS service port for login to the device. Moreover, configure redirection to HTTPS when accessing through HTTP. Thus, the Web browser can access the Web server through either HTTP or HTTPS.

4. Procedure

Configure the management IP address on the device to make the device reachable to the server via L3 routes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 1.1.1.1 255.255.255.0
```

Enable both the HTTP and HTTPS services.

```
Hostname(config)# enable service web-server
```

Set the HTTP service port number to 8080.

```
Hostname(config)# http port 8080
```

Set the HTTPS service port number to 4430.

```
Hostname(config)# http secure-port 4430
```

Configure the HTTP authentication information.

```
Hostname(config)# webmaster level 1 username test1 password 0 test_password1
```

Configure HTTP redirection to HTTPS.

```
Hostname(config)# web-server http redirect-to-https
```

Configure the device to generate a self-signed certificate again.

```
Hostname# configure terminal
Hostname(config)# web-server https generate self-signed-certificate
RSA key modulus bits (1024~4096) [2048]:
Common Name (e.g. server IP) [Self-Signed-600B16C2]:
% Generate self-signed certificate successfully
```

5. Verification

Run the **ping** command to check whether the L3 route between the server and the server is reachable.

```
Hostname# ping 1.1.1.10
Sending 5, 100-byte ICMP Echoes to 1.1.1.10, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/2 ms.
```

Run the **show web-server status** command to display the configuration of the HTTP service.

```
Hostname# show web-server status
http server status: enabled
http server port: 8080
https server status:enabled
https server port: 4430
```

Run the **show web-server status** command to check whether HTTP redirection to HTTPS is enabled. When **http redirect to https** is **true**, the feature is enabled.

```
Hostname# show web-server status
http server status : enabled
http server port: 8080
```

```
https server status: enabled
https server port: 4343
http redirect to https: true
```

Run the **show web-server https certificate information** command to display the certificate information.

```
Hostname# show web-server https certificate information
Source: Default
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Self-Signed-93610DFD
        Validity
            Not Before: Apr  7 02:05:02 2020 GMT
            Not After : Apr  5 02:05:02 2030 GMT
        Subject: CN=Self-Signed-93610DFD
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:fb:de:8e:c0:f8:0d:53:ff:c1:57:a0:82:32:23:
                    41:d9:1c:c3:95:8e:02:a7:d7:5d:20:86:bb:bc:8f:
                    42:40:22:ef:9b:03:53:40:bf:16:fd:b7:ec:07:61:
                    78:8a:21:6c:4b:27:91:43:c4:5c:72:e5:df:bc:0e:
                    8a:d7:8f:e9:61:9b:77:22:4c:6e:e1:bf:cd:d6:9b:
                    f6:0d:ce:4e:32:b4:e4:e7:74:9b:fc:1d:45:a4:41:
                    5a:0f:6b:2e:b7:a3:ff:93:2e:f3:6b:67:b0:9e:89:
                    55:eb:ac:a2:ab:1f:b1:bc:24:4a:c2:87:ba:db:06:
                    09:22:b2:51:ae:6e:79:6b:c7:cb:16:25:d3:9a:6f:
                    41:99:b3:da:51:5d:39:21:aa:d2:45:44:79:40:78:
                    76:aa:1d:e0:3f:b3:ee:7a:ac:5b:8a:c6:96:c2:01:
                    57:60:83:16:b6:5c:55:d6:38:20:28:26:28:60:8c:
                    51:7b:3f:08:c1:f1:1b:1e:8d:58:b9:e9:c3:00:0c:
                    9d:6f:12:6a:97:67:70:61:1b:64:48:c3:2d:22:43:
                    15:51:3c:6c:24:15:66:bd:85:3b:4b:f0:bc:94:eb:
                    ef:f6:c0:5c:d1:54:1e:1f:84:72:9c:45:82:8f:e3:
                    83:26:a6:fe:72:d6:5f:32:27:93:ac:ae:a6:f4:d0:
                    d4:77
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
    Signature Algorithm: sha256WithRSAEncryption
         df:d2:8a:81:bf:d7:6b:23:1e:d9:a2:2c:48:35:ee:82:b0:33:
         c2:eb:a3:be:3f:78:57:39:6a:f1:ce:f2:ce:85:60:22:22:5c:
         94:b9:f2:d3:07:8e:f2:6b:7e:8f:b6:7b:5b:08:20:7a:73:e3:
```

```
        96:42:9d:9d:b9:11:39:2c:41:eb:fb:c7:57:87:6e:85:67:b5:
        35:a4:9b:04:43:8b:97:f5:66:80:e1:31:fb:ef:3c:74:59:2b:
        5b:77:6c:9d:9e:59:a8:3e:95:28:f8:76:97:b6:5a:d0:8e:4e:
        d0:e2:69:89:df:ba:a0:c3:12:39:f3:77:92:66:f6:d0:49:4a:
        e1:d2:df:01:d3:90:03:57:8d:2a:ef:ff:5c:b0:8a:6b:32:e0:
        84:bb:54:99:5f:0a:c5:6f:ff:4d:7d:8f:52:a7:ed:b2:f5:79:
        bd:20:f8:13:2a:05:d0:10:49:48:3d:72:b2:b1:f5:89:32:aa:
        f8:bd:76:f3:af:d9:59:8c:06:fe:4d:0d:d4:66:47:d2:c2:f4:
        bd:16:93:6c:31:1e:3a:8e:2c:3c:bc:af:81:3f:50:7f:8c:74:
        a1:90:a8:ea:34:29:7f:53:32:57:a9:cb:c3:a1:c7:0f:4a:97:
        c1:18:88:ab:cf:0c:c9:60:64:4e:42:25:dc:9d:e7:d0:5b:35:
        e8:23:30:dd
```

6. Configuration Files

```
hostname Device
!
ip name-server 1.1.1.1
!
http port 8080
http secure-port 4430
enable service web-server http
enable service web-server https
web-server http redirect-to-https
webmaster level 0 username admin secret 8
$1c$7eyy23uMQk$!b(`dhh`n<nxlvxn&tp8$.<h!dfp46#2rlzj>x#h$
!
interface GigabitEthernet 0/1
 no switchport
 ip address 1.1.1. 255.255.255.0
```

7. Common Errors

If the HTTP service port is not the default port 80 or 443, you must enter a specific configured service port in the browser. Otherwise, you cannot access the device in Web mode.

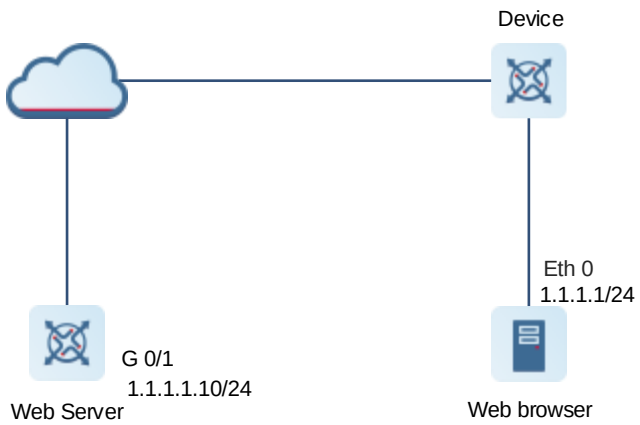
1.6.2 Configuring Remote HTTP Upgrade

1. Requirements

To reduce the impact on network communications, perform upgrade early in the morning. Therefore, you can use the remote HTTP upgrade feature to upgrade the device using files.

2. Topology

Figure 1-3 Topology for Remote HTTP Upgrade



3. Notes

- Configure L3 route reachable between the server and the device.
- Enable the HTTP service.
- Before configuring the domain name of an HTTP upgrade server, enable DNS on the device and configure the DNS server address.
- The device obtains upgrade files from the Web server at 02:00 every day, and downloads the latest upgrade files to upgrade itself.

4. Procedure

Configure the management IP address on the device to make the device reachable to the server via L3 routes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 1.1.1.1 255.255.255.0
```

Configure the DNS.

```
Hostname(config)# ip domain-lookup
Hostname(config)# ip name-server 192.168.58.110
```

Enable the HTTP service.

```
Hostname(config)# enable service web-server
```

Set the scheduled time for the device to start remote monitoring to 02:00.

```
Hostname(config)# http update time daily 02:00
```

Configure the device to obtain upgrade files from the remote server.

```
Hostname# http check-version
```

Configure the device to download upgrade files from the server and update the device.

```
Hostname# http update all
```

5. Verification

Run the **ping** command to check whether the L3 route between the server and the server is reachable.

```
Hostname# ping 1.1.1.1
Sending 5, 100-byte ICMP Echoes to 1.1.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/2 ms.
```

6. Configuration Files

```
hostname Device
!
ip name-server 1.1.1.1
!
enable service web-server http
enable service web-server https
webmaster level 0 username admin secret 8
$1c$7eyy23uMQk$!b(`dhh`n<nxlvxn&tp8$.<h!dfp46#2rlzj>x#h$
http update time daily 02:00
!
interface GigabitEthernet 0/1
 no switchport
 ip address 1.1.1. 255.255.255.0
```

7. Common Errors

DNS is disabled, so the device cannot establish a connection with the server.

Contents

1 Configuring Syslog 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Classification of System Logs 1
1.1.3 Levels of System Logs 1
1.1.4 Output Direction of System Logs 2
1.1.5 RFC5424 Log Format 2
1.1.6 System Log Filtering 4
1.1.7 Log Reporting 5
1.1.8 Configuring System Log Monitoring 6
1.1.9 Protocols and Standards 6
1.2 Configuration Task Summary 6
1.3 Configuring Basic Syslog Features 7
1.3.1 Overview 7
1.3.2 Procedure 7
1.4 Configuring the System Log Format 7
1.4.1 Overview 7
1.4.2 Restrictions and Guidelines 7
1.5 Configuring Log Reporting 8
1.5.1 Configuration Tasks 8
1.5.2 Restrictions and Guidelines 8
1.5.3 Configuring Level-based Log Reporting 8

1.5.4 Configuring Delayed Log Reporting 8

1.5.5 Configuring Periodical Log Reporting 10

1.6 Configuring System Log Monitoring 11

1.6.1 Overview 11

1.6.2 Restrictions and Guidelines 11

1.6.3 Procedure 11

1.7 Configuring the Output Direction of System Logs 12

1.7.1 Configuration Tasks 12

1.7.2 Configuring the Output of System Logs to the Console 12

1.7.3 Configuring the Output of System Logs to the Monitor Terminal 13

1.7.4 Configuring the Function of Writing System Logs into the Memory Buffer 13

1.7.5 Configuring the Transmission of System Logs to the Log Server 14

1.7.6 Configuring the Function of Writing System Logs into Log Files 15

1.8 Configuring System Log Filtering 17

1.8.1 Overview 17

1.8.2 Restrictions and Guidelines 17

1.8.3 Procedure 17

1.9 Configuring System Log Redirection 17

1.9.1 Overview 17

1.9.2 Restrictions and Guidelines 18

1.9.3 Procedure 18

1.10 Configuring Performance Logging Function 18

1.10.1 Overview 18

1.10.2 Restrictions and Guidelines 18

1.10.3 Procedure....18

1.11 Configuring Synchronization of User Input and Log Output....19

1.11.1 Overview....19

1.11.2 Restrictions and Guidelines....19

1.11.3 Procedure....19

1.12 Monitoring....19

1.13 Configuration Examples....20

1.13.1 Configuring the RFC5424 Log Format....20

1 Configuring Syslog

1.1 Introduction

1.1.1 Overview

If link status change or events such as receiving of exception packets and processing exception occur during the device running, a log packet in a fixed format is generated automatically. A log packet can be added with a timestamp and a sequence number, classified by the log priority, and output to the console, monitor terminal, log server, or other media. Logs are used by administrators to monitor the running status of the device, analyze the network conditions, and locate problems.

1.1.2 Classification of System Logs

System logs fall into two types:

- Common logs
- Debugging logs

Note

To generate debugging logs, you need to enable a debug command. Such logs are used to locate problems, and may be ignored by users.

1.1.3 Levels of System Logs

Eight severity levels are defined for system logs in a descending order, including emergency, alert, critical, error, warning, notification, informational, and debugging, which correspond to eight numerical values from 0 to 7 respectively. A smaller value indicates a higher level. Table 1-1 describes the log levels.

Note

Only logs with a level equal to or higher than the specified level are output. For example, if the level of logs is set to informational (level 6), logs of level 6 or higher are output.

Table 1-1 Description of Log Levels

Keyword	Level	Description
emergencies	0	Indicates that the system cannot run normally.
alerts	1	Indicates that corrective measures must be taken immediately.
critical	2	Indicates a critical circumstance.
errors	3	Indicates an error message.
warnings	4	Indicates a warning.

Keyword	Level	Description
notifications	5	Indicates a common but important message that requires attention.
informational	6	Indicates an informational message.
debugging	7	Indicates debugging information.
emergencies		

1.1.4 Output Direction of System Logs

System logs can be output to the console, monitor, server, buffer, and file. The default level and type of logs vary with the output direction. You can customize filtering rules for different output directions. Table 1-2 describes output directions of system logs.

Table 1-2 Description of System Log Output Directions

Name of Output Direction	Default Output Direction	Default Output Level	Description
console	Console	debugging (Level 7)	Outputs logs and debugging information.
monitor	Monitor terminal	debugging (Level 7)	Outputs logs and debugging information to facilitate remote maintenance.
server	Log server	informational (Level 6)	Outputs logs and debugging information.
buffer	Log buffer	debugging (Level 7)	Outputs logs and debugging information. The log buffer is used to store system logs during the device running.
file	Log file	informational (Level 6)	Outputs logs and debugging information, and periodically writes logs in the log buffer into files.

1.1.5 RFC5424 Log Format

All system logs are in the following format regardless of their output directions:

```
<priority>version timestamp sysname MODULE LEVEL MNEMONIC [structured-data]
description
```

The log format is described below:

<Priority>version timestamp system name module name level mnemonic structured parameter area log content

For example, if you exit the configuration mode, the following log is displayed on the console:

```
<133>1 2013-07-24T12:19:33.130290Z ruijie SYS 5 CONFIG - Configured from console by console
```

The following details each field:

- priority

  The priority is calculated using the following formula: Facility × 8 + Level. "Level" indicates the log level and "Facility" indicates the facility value. The facility value can be set during log configuration. When the RFC5424 log function is enabled, the default facility value is local0 (16).

- version

  According to RFC5424, the version is always **1**.

- timestamp

  The timestamp records the generation time of a system log to help you check and locate system events. Ruijie devices use the following uniform timestamp format when the RFC5424 logging function is enabled:

  ```
  YYYY-MM-DDTHH:MM:SS.SECFRACZ
  ```

  Table 1-3 describes each parameter.

Table 1-3 Description of Timestamp Parameters

Timestamp Parameter	Parameter Name	Description
YYYY	Year	Indicates the year.
MM	Month	Indicates the month in the current year.
DD	Day	Indicates the day in the current month.
T	Separator	A date must end with "T".
HH	Hour	Indicates the hour.
MM	Minute	Indicates the minute.
SS	Second	Indicates the second.
SECFRAC	Millisecond	Indicates the millisecond (1–6 digits).
Z	End mark	Time must end with "Z".

- sysname (system name)

  This field indicates the name of the device that generates a log so that the log server can identify the host of such device.

- MODULE (module name)

  This field indicates the name of the module that generates a log. The value is an upper-case string of 2 to 20 characters, which can contain upper-case letters, digits, and underscores. The **module** field is mandatory for common logs by default, and optional for debugging logs.

- LEVEL (log level)

Eight system log levels from 0 to 7 are defined. The level of system logs generated by each module is determined during development and cannot be changed.

- MNEMONIC

  This field indicates a summary of the generation of a log. The value is an upper-case string of 4 to 32 characters, which can contain upper-case letters, digits, and underscores. The **mnemonic** field is mandatory for common logs by default, and optional for debugging logs.

- structured-data (structured parameter area)

  This field is introduced to RFC5424, to describe log parameters in a way that helps device parsing. Each log can contain 0 or multiple parameters. If no parameter exists, the placeholder (-) must be used. Each parameter is in the following format:

```
[SD_ID@enterpriseID PARAM-NAME=PARAM-VALUE]
```

  Table 1-4 describes each parameter.

Table 1-4 Description of Structured Parameters

Structured Parameter	Parameter Name	Description
SD_ID	Name of parameter information	The name of parameter information is capitalized, and must be unique in a log.
@	Separator	"@enterpriseID" is necessary for the customized parameters, but not for parameters defined in RFC5424.
enterpriseID	Enterprise ID	The enterprise ID is maintained by the Internet Assigned Numbers Authority (IANA). The enterprise ID of Ruijie devices is 4881. You can query the enterprise ID at the official website of IANA.
PARAM-NAME	Parameter name	The parameter name is capitalized, and must be unique in the structured parameter area of a log.
PARAM-VALUE	Parameter value	The parameter value must be enclosed in double quotation marks. Values of the IP address and MAC address must be capitalized, and values of other parameters are capitalized as required.

- description (log text)

  This field indicates the content of a system log.

1.1.6 System Log Filtering

By default, the logs generated by the system are output in all directions. The device provides the log filtering function, which allows you to filter logs by log output direction, log keyword, and matching rule. When you do not care about some logs or you care about some logs only, use the log filtering function to filter the logs.

- Filtering direction

  Four log filtering directions are defined:

- **buffer**: Filters the logs sent to the log buffer, that is, the logs displayed by the **show logging** command.
- **file**: Filters the logs written into logging files.
- **server**: Filters the logs sent to the log server.
- **terminal**: Filters the logs sent to the console and monitor terminal (including telnet and SSH).

Note

The four filtering directions can be used either collectively (logs in various directions are filtered) or separately (logs in one direction are filtered).

- Filtering Mode

  Two filtering modes are available:

  - **contains-only**: Indicates that only the logs that contain keywords specified in the filtering rules are output. When you care about some logs only, you can apply the contains-only mode on the device to output only the logs that match the filtering rules on the terminal. Thus, you can check whether any event occurs.
  - **filter-only**: Indicates that the logs that contain keywords specified in the filtering rules are filtered and are not output. Too many logs from a module may result in spamming on the terminal CLI . If you do not care about this type of logs, you can apply the filter-only mode and configure filtering rules to filter such logs.

Note

The two filtering modes are mutually exclusive, that is, you can configure only one filtering mode at a time.

- Filtering Rule

  Two log filtering rules are available:

  - **exact-match**: If exact-match is selected, you must select all the three filtering options (log module, log level, and log mnemonic). To filter a specific log, use the exact-match filtering rule.
  - **single-match**: If single-match is selected, you only need to select one of the three filtering options (log module, log level, and log mnemonic). To filter a specified type of log, use the single-match filtering rule.

Note

If the same module name, log level, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule prevails.

1.1.7 Log Reporting

The log reporting functions falls into level-based reporting, delayed reporting, and periodical reporting, which are described as follows:

- Level-based reporting

  You can perform the level-based policy function to send logs of modules and severity levels to different destinations.

For example, you can configure a command to send OSPF module logs of level 4 or lower to the log server, and OSPF module logs of level 5 or higher to local log files.

- Delayed reporting

  Delayed log reporting means that instead of being directly sent to the log server, system logs generated in the system are buffered in the log files in the device and then periodically sent to the log server. Delayed log reporting can be configured to reduce the packet transmission and interaction frequency between the device and the log server. In this way, the performance pressure on the device and the log server and the burden of the intermediate network is reduced.

- Periodical reporting

  Logs about device performance statistics are periodically sent. All timers for periodically sending logs are managed by the syslog module. When a timer expires, the syslog module calls the log processing function registered by each module to display and output the performance statistic logs to the remote syslog server in real time. The server analyzes these logs to evaluate the device performance.

Caution

- To configure log reporting, enable the RFC5424 log format function; otherwise, you cannot configure level-based reporting, delayed reporting, and periodical reporting.
- When the RFC5424 log format is enabled, logs can be output in all directions, and delayed reporting is enabled by default. At the same time, the periodical reporting function is disabled.

1.1.8 Configuring System Log Monitoring

System log monitoring means that the system monitors external connections to the device and records logs.

- After user login/logout logging is enabled, the system records the user's connections to the device. The recorded information includes the login username and source address.
- After user operation logging is enabled, the system records device configuration changes. The recorded information includes the operation username, source address, and operation content.

1.1.9 Protocols and Standards

- RFC 3164: The BSD syslog Protocol
- RFC 5424: The_Syslog_Protocol

1.2 Configuration Task Summary

Syslog configuration includes the following tasks:

(1) Configuring Basic Syslog Features

(2) (Optional) Configuring the System Log Format.

(3) Configuring Log Reporting Configure at least one of the functions.

- Configuring Level-based Log Reporting
- Configuring Delayed Log Reporting
- (Optional) Configuring Periodical Log Reporting

(4) (Optional) Configuring System Log Monitoring

(5) (Optional) Configuring the Output Direction of System Logs. Configure at least one of the output directions.

- Configuring the Output of System Logs to the Console
- Configuring the Output of System Logs to the Monitor Terminal
- Configuring the Function of Writing System Logs into the Memory Buffer
- Configuring the Transmission of System Logs to the Log Server
- Configuring the Function of Writing System Logs into Log Files

(6) (Optional) Configuring System Log Filtering

(7) (Optional) Configuring System Log Redirection

(8) (Optional) Configuring Performance Logging Function

(9) (Optional) Configuring Synchronization of User Input and Log Output

1.3 Configuring Basic Syslog Features

1.3.1 Overview

This section describes how to enable the syslog function so that the system processes logs and users view the logs generated by the device.

1.3.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable logging.

logging on

By default, logging is enabled.

1.4 Configuring the System Log Format

1.4.1 Overview

By configuring system log display, you can adjust the display format of system logs.

1.4.2 Restrictions and Guidelines

- After the RFC5424 log format is enabled, a uniform timestamp format is adopted, and **uptime** and **datetime** are not differentiated.
- In the RFC5424 log format, the timestamp may or may not contain the time zone. Currently, only the timestamp without the time zone is supported.

1. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the system log format to the RFC5424 log format.

service log-format rfc5424

1.5 Configuring Log Reporting

1.5.1 Configuration Tasks

The log reporting configuration includes the following tasks. Configure at least one of the tasks.

- Configuring Level-based Log Reporting
- Configuring Delayed Log Reporting
- (Optional) Configuring Periodical Log Reporting

1.5.2 Restrictions and Guidelines

The log reporting function can be configured and takes effect only when the RFC5424 format is enabled.

1.5.3 Configuring Level-based Log Reporting

1. Overview

You can configure a level-based log reporting policy to output logs of different modules and severity levels to different destinations.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the system log format to the RFC5424 log format.

service log-format rfc5424

(4) Configure a level-based log reporting policy.

logging policy module *module-name* [**not-lesser-than**] *policy-level* **direction** { **all** | **buffer** | **console** | **file** | **monitor** | **server** }

No level-based log reporting policy is configured by default.

1.5.4 Configuring Delayed Log Reporting

1. Overview

Delayed log reporting means that, instead of being directly sent to the log server, system logs generated in the system are buffered in the log files in the device and then periodically sent to the log server. Delayed log reporting can be configured for system logs to reduce the message transmission and interaction frequency between the device and the log server. In this way, the performance pressure on the device and the syslog server and the burden of the intermediate network is reduced.

2. Restrictions and Guidelines

- Generally, you are not advised to output logs reported in a delayed manner to the console or remote terminal. Otherwise, many logs reported in a delayed manner are displayed, increasing the burden on the device.
- The configured file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (**.txt**) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by the file system of your PC, such as \, /, :, *, ", <, >, and |. For example, the configured file name is **log_server**, the current index is 5, the file size is 1000 bytes, and the source IP address of the device sending the log file is 10.2.3.5. The name of the log file sent to the remote server is **log_server_1000_10.2.3.5_5.txt** while the name of the log file stored on the device is **log_server_5.txt**. If the source IP address is an IPv6 address, the colon (:) in the IPv6 address must be replaced by the hyphen (-) because the colon (:) is prohibited by the file system. For example, the file name is **log_server**, the current file index is 6, the file size is 1000 bytes, and the source IPv6 address of the device sending the log file is 2001::1. The name of the log file sent to the remote server is **log_server_1000_2001-1_6.txt** while the name of the log file stored on the device is **log_server_6.txt**.
- If few logs are generated on the device, you are advised to set the interval of delayed log reporting to a large value so that more logs are sent to the remote server at a time.
- By default, the log file sent to the remote server is named **File size_device IP address_index.txt**. If the name of the file for delayed log reporting is modified, the log file sent to the remote server is named **Configured file name prefix_file size_device IP address_index.txt**. The file stored on the local flash space of the device is named **Configured file name prefix_index.txt**. The default file name prefix is **syslog_ftp_server**, the interval for delayed log reporting is 3600s (1 hour), and the log file size is 128 KB.
- The maximum interval for delayed log reporting is 65535s (18 hours). If you set the interval for delayed log reporting to a larger value, the size of logs generated in this period may exceed the file size (128 KB). To prevent loss of logs, the logs are written into a new log file, and the index increases by 1. When the timer expires, all log files buffered in this period are sent to the log server at a time.
- The flash space for buffering local log files on the device is limited. Therefore, up to eight log files are buffered on the device. If more than eight log files are buffered on the device, all the log files generated earlier are sent to the log server at a time.
- You can send logs to the log server through File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP). The addresses of up to five log servers are configured for one device. Either FTP or TFTP is specified for each server.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the system log format to the RFC5424 log format.

service log-format rfc5424

(4) Configure delayed log reporting. The following configurations are optional. Configure at least one of them as actually needed.

- Configure delayed log reporting to the console and remote terminal.

  logging delay-send terminal

  Delayed log reporting to the console and remote terminal is disabled by default.

- Configure the name of the file for delayed log reporting.

  logging delay-send file flash: *delay-send-filename*

  The default format of the log file name is file size_device IP address_index.txt.

- Configure the interval for delayed log reporting.

  logging delay-send interval *delay-send-interval*

  The interval for delayed log reporting is 3600s (1 hour) by default.

- Configure the server address and reporting mode.

  logging delay-send server [**oob**] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**via** *mgmt-name*] **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }

  Delayed log reporting is disabled by default.

1.5.5 Configuring Periodical Log Reporting

1. Overview

This section describes how to configure periodical log reporting so that the server can collect all the logs on the device at the same time point.

2. Restrictions and Guidelines

- The interval of periodical log reporting and the function of outputting logs to the console and remote terminal take effect only after periodical log reporting is enabled.
- You are advised to disable the function of outputting periodically reported logs to the console and remote terminal. Otherwise, when the reporting timer expires, many performance statistics logs are displayed, increasing the burden on the device.
- To ensure that the server collects all performance statistics logs from the device at the same time point, the timers of all statistical objects are restarted when you modify the interval of one statistic object.
- The default interval of periodical log reporting is 15 minutes. To enable the server to collect all performance statistics logs from the device at the same time point, you need to set the log reporting interval of different statistic objects to be a multiple of another interval . Currently, the interval can be set to 0, 15, 30, 60, or 120. Here, **0** indicates that periodical log reporting is disabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the system log format to the RFC5424 log format.

service log-format rfc5424

(4) Configure periodical log reporting.

logging statistic enable

Periodical log reporting is disabled by default.

(5) (Optional) Configure periodical log reporting to the console and remote terminal.

logging statistic terminal

Periodical log reporting to the console and remote terminal is disabled by default.

(6) (Optional) Configure the interval for periodical log reporting.

logging statistic mnemonic *mnemonic* **interval** *logging-statistic-interval*

The default interval of periodical log reporting is 15 min.

1.6 Configuring System Log Monitoring

1.6.1 Overview

System log monitoring enables the system to monitor the external connections to the device and record logs.

1.6.2 Restrictions and Guidelines

- If both the **logging userinfo** command and the **logging userinfo command-log** command are configured on the device, only the results shown by the **logging userinfo command-log** command are displayed when you run the **show running-config** command.
- The **logging userinfo** command is run in global configuration mode to enable login/logout logging. After this function is configured, the device displays logs when users access the devices through telnet, Secure Shell (SSH), or Hypertext Transfer Protocol (HTTP) so that the administrator monitors the device connection status.
- The **logging userinfo command-log** command is run in global configuration mode to enable user operation logging. After this function is configured, the system displays related logs to notify the administrator of configuration changes.
- User operations are logged when commands are configured and run. By default, the device does not generate operation logs when a user modifies the device configuration. If the 5424 log format is configured, that is, the **service log-format rfc5424** command is configured, you need to configure the **logging delay-send terminal** command so that operation logs are output to the terminal (because delayed log reporting is registered for operation logs).

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure system log monitoring. The following configurations are all optional. Configure at least one of them as actually needed.

- Enable user login/logout logging.

  logging userinfo

  User login/logout logging is disabled by default.

- Enable user operation logging.

  logging userinfo command-log

  User operation logging is disabled by default.

1.7 Configuring the Output Direction of System Logs

1.7.1 Configuration Tasks

System log output direction configuration includes the following tasks. Configure at least one of the tasks.

- (Optional) Configuring the Output of System Logs to the Console
- (Optional) Configuring the Output of System Logs to the Monitor Terminal
- (Optional) Configuring the Function of Writing System Logs into the Memory Buffer
- (Optional) Configuring the Transmission of System Logs to the Log Server
- (Optional) Configuring the Function of Writing System Logs into Log Files

1.7.2 Configuring the Output of System Logs to the Console

1. Overview

This section describes how to configure the output of system logs to the console so that the device can output logs generated by the system to the console. Then, administrator can monitor the running status of the system.

2. Restrictions and Guidelines

- If too many system logs are generated, you can limit the logging rate to reduce logs output to the console.
- By default, system logging is enabled. You are advised not to disable it. If too many system logs are displayed, you can configure the level of logs to be displayed on different devices to reduce the logs displayed.
- The **logging count** command is run to enable the log statistics function in global configuration mode. After this function is enabled, the system records the number of times logs are generated by each module and the generation time of the last log.
- The default level of logs that are displayed on the console is debugging (Level 7). You can run the **show logging config** command in privileged EXEC mode to display the level of logs that are displayed on the console.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable log statistics collection.

logging count

Log statistics collection is disabled by default.

(4) (Optional) Configure the level of logs that are output to the console.

logging console [*severity-level*]

The default level of logs that are displayed on the console is 7 (debugging information).

(5) (Optional) Configure logging rate limiting.

logging rate-limit { *number* | **all** *number* | **console** { *number* | **all** *number* } } [**except** [*severity-level*]]

Logging rate limiting is disabled by default.

1.7.3 Configuring the Output of System Logs to the Monitor Terminal

1. Overview

This section describes how to configure the output of system logs to the monitor terminal so that the device can output system logs to the remote monitor terminal. Then, the administrator can monitor the running status of the system.

2. Restrictions and Guidelines

- If too many system logs are generated, you can limit the logging rate to reduce logs output to the monitor terminal.
- By default, the current monitor terminal is not allowed to output logs after you remotely connect to the device. You need to manually run the **terminal monitor** command to allow the current monitor terminal to display logs. The **terminal monitor** command is valid only for the current connection. When the terminal reconnects to the device, the default settings of this command are restored**.**

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enable log display on the current monitor terminal.

terminal monitor

Log display in the window of the monitor terminal is disable by default.

(3) Enter the global configuration mode.

configure terminal

(4) (Optional) Configure the level of logs to be output to the monitor terminal.

logging monitor [*severity-level*]

The default level of logs that are displayed in the window of the monitor terminal is 7 (debugging information).

1.7.4 Configuring the Function of Writing System Logs into the Memory Buffer

1. Overview

This section describes how to configure the function of writing system logs into the memory buffer so that the device can write generated system logs into the memory buffer. Then, the administrator can view recent system logs by running the **show logging** command.

2. Restrictions and Guidelines

- If the buffer is full, earlier logs are overwritten when system logs are written into the memory buffer.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the parameters for the memory buffer, into which logs are to be written.

logging buffered [*buffer-size*] [*severity-level*]

The buffer size is 1 mega-byte and the log severity level is 7 by default.

1.7.5 Configuring the Transmission of System Logs to the Log Server

1. Overview

This section describes how to configure the device to transmit generated system logs to the log server so that the administrator can monitor device logs on the server.

2. Restrictions and Guidelines

- The log timestamp or sequence number function must be enabled. Otherwise, the logs are not sent to the log server.
- If the device has an MGMT interface and is connected to the log server through the MGMT interface, you must add the **oob** option (indicating that system logs are sent to the log server through the MGMT interface) when configuring the **logging server** command. You can use the **via** parameter only when **oob** is specified in the command. In this case, **/vrf** is unavailable.
- The **logging server** command is used to specify the address of the log server that receives logs. You can specify multiple log servers, and logs are sent simultaneously to all these log servers.
- Up to five log servers are configured for a Ruijie product.
- When a domain name is entered to configure a log server, the **logging hostname** command is disabled.
- To track and manage logs, you can use the **logging source interface** command to set the source IP address of all log packets to the IP address of an interface. Thus, the administrator can identify the device that sends the logs based on the unique address. If this source interface is not configured or the IP address is not configured for this source interface, the source IP address of log packets is the IP address of the interface that sends the log packets.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the transmission of logs to a specified log server.

(4) **logging { server** [**oob**] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**via** *mgmt-name*] [**udp-prot** *port-number*] [**vrf** *vrf-name*] [**facility** *facility-type*] [**level** *inform-level*] | { *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**udp-prot** *port-number*] [**facility** *facility-type*] [**level** *inform-level*] }(Optional) Configure the level of logs that are sent to the log server.

logging trap [*severity-level*]

The default level of logs that are sent to the log server is 6 (informational messages).

(5) (Optional) Configure the facility value for logs to be sent to the log server.

logging facility *facility-type*

When the RFC5424 log format is enabled, the default facility value is 16 (Local0, Local use); when the RFC5424 log format is disabled, the default facility value is 23 (Local7, Local use).

(6) (Optional) Configure the source interface for logs to be sent to the log server.

logging source interface *interface-type interface-number*

No log source address is configured by default, and the source IP address of the log packets sent to the server is the IP address of the interface that sends the log packets.

(7) (Optional) Configure the source address for logs to be sent to the log server.

- Configure an IPv4 source address for the logs to be sent to the log server.

  logging source ip *ipv4-address*

- Configure an IPv6 source address for the logs to be sent to the log server.

  logging source ipv6 *ipv6-address*

No log source address is configured by default, and the source IP address of the log packets sent to the server is the IP address of the interface that sends the log packets.

1.7.6 Configuring the Function of Writing System Logs into Log Files

1. Overview

This section describes how to configure the function of writing system logs into log files so that the device can save generated system logs to the log files for viewing. Logs are saved in a log file buffer before being saved to the log file. The system writes the content in the log file buffer to the log file at the specified frequency, and you can also save the logs to a log file manually. After the logs are saved, the content in the log file buffer will be cleared. When logs need to be saved, the device automatically generates log files.

2. Restrictions and Guidelines

- System logs are not immediately written into log files. They are first buffered in the memory buffer, and then written into log files either periodically (at an interval of 1 hour by default) or when the buffer is full.
- When no log file is generated and the remaining space of the storage medium is insufficient, the device does not save the newly generated logs to a log file. Therefore, you must regularly clean up the storage space of the storage medium to ensure the log file function.
- The **logging file** command is used to create a log file with a specified file name on a specified file storage device. The file size increases with logs, but cannot exceed the configured value of **max-file-size**. If the value of **max-file-size** is not specified, the default size of a log file is 128 KB.
- After the **logging file** command is configured, the system saves logs to log files. A log file name does not contain any file type extension. The log file name extension is always **txt**, which cannot be changed.
- After this function is configured, logs will be written into log files at an interval of 1 hour. If you have run the **logging file flash:syslog** command, 16 log files are created, such as **syslog.txt**, **syslog_1.txt**, **syslog_2.txt**, …, **syslog_14.txt**, and **syslog_15.txt**. Logs are overwritten into the 16 log files in sequence and cyclically. For example, the system writes logs into **syslog_1.txt** after **syslog.txt** is fully occupied.

When **syslog_15.txt** is fully occupied, logs are written into **syslog.txt** again.

- If no extended flash space is available, the **logging file flash** command is automatically hidden and is not configured. If no FLASH2 is available, the **logging file flash2** command is automatically hidden and is not configured. If FLASH2 is available and the **logging file flash** command is configured, logs are recorded in FLASH2.
- The system will not delete the generated log files after the number of log files is modified. Therefore, to save the space of the extended flash space, you need to manually delete the log files generated in the system (before deletion, you can transfer the log files to an external server through TFTP). For example, 16 log files are created by default after the function of writing logs into log files is enabled. If the device has generated 16 log files and if you want to change the number of log files to 2, new logs are overwritten into the log files with the index of 0 and 1 by turns. The existing log files with the index of 2 to 16 are retained. You can manually delete these log files as needed.
- After the time-based log storage is enabled, the system writes logs of the same level that are generated in the same day into the same log file. The log file is named **yyyy-mm-dd_filename_level.txt**, where **yyyy-mm-dd** indicates the absolute time of the day when the logs are generated, **filename** indicates the log file name configured by the **logging file flash** command, and **level** indicates the log level.
- After you specify the storage time for logs of a level, the system will delete the logs once the storage time expires. For better network management, the storage time ranges from 7 days to 365 days.
- If the time-based log storage is not enabled, logs are stored based on the file size to support old configuration commands.
- After the **logging flash flush** command is configured, the logs in the buffer are immediately written into a log file.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the parameters for the log file, into which logs are written.

logging file { | **flash:***filename* | **usb0**:*filename* } [*max-file-size*] [*inform-level*]

(4) Configure the number of log files.

logging file numbers *file-numbers*

The default number of log files is 16.

(5) Configure the interval for writing logs into log files.

logging flash interval *log-write-flash-interval*

By default, logs are written into flash files at an interval of 3600s.

(6) Configure the storage time of logs written into log files.

logging life-time level *inform-level life-time-days*

No storage time is configured by default. The storage time depends on the configured log file size.

(7) Configure the function of immediately writing logs in the buffer into log files.

logging flash flush

1.8 Configuring System Log Filtering

1.8.1 Overview

By default, all the logs generated by the system are displayed on the console or other terminals. By configuring log filtering, the network administrator can filter the generated system logs, select only the required logs to be displayed, or have the logs displayed on a specified terminal.

1.8.2 Restrictions and Guidelines

- Two filtering modes are available: **contains-only** and **filter-only**, which are mutually exclusive. You can configure only one filtering mode at a time.
- Log filtering rules fall into **exact-match** and **single-match**. The **single-match** rule prevails over the **exact-match** rule. If the same module, mnemonic, or information level is configured in both the **single-match** and **exact-match** rules, the logs complying with the **single-match** rule are filtered first.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the log filtering direction. The following configurations are optional. Select at least one of the configurations as actually needed.

- Configure the log filtering direction.

  logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }

  Logs sent to all the directions are filtered by default, namely, **all** is set.

- Configure the log filtering mode.

  logging filter type { **contains-only** | **filter-only** }

  The filtering type is set to **filter-only** by default.

(4) Configure the log filtering rule.

logging filter rule { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *inform-level* | **single-match** { **level** *inform-level* | **mnemonic** *mnemonic-name* | **module** *module-name* } }

No log filtering rule is configured by default.

1.9 Configuring System Log Redirection

1.9.1 Overview

In a virtual switching unit (VSU) environment, you can configure the system log redirection function to redirect the logs of the slave device to the active device so that the network administrator can manage the logs uniformly.

1.9.2 Restrictions and Guidelines

- The system log redirection function is used in a VSU active-standby environment only, and does not apply to the standalone environment.
- You are advised to run the **logging rd rate-limit** command to limit the rate of the logs redirected to the active device. This is to limit the number of the logs that are redirected from the slave device to the active device per second. This prevents considerable logs on the slave device from burdening the system.
- In a VSU environment, logs on the slave device can be displayed in its console window, redirected to the active device for display in the console or virtual type terminal (VTY) window of the active device, or stored in the memory buffer of the active device, extended flash space or syslog server.
- In a VSU environment composed of box-type devices, after the log redirection function is enabled, logs on the slave or standby device will be redirected to the active device for output, and the role flag string "(*device ID)" will be added to the beginning of each log, to indicate that the log is a redirected log. Assume that four devices form a VSU. The ID of the active device is 1, the ID of the slave device is 2, and the IDs of two standby devices are 3 and 4. No role flag string is added to logs generated by the active device. The role flag string (*2) is added to logs redirected from the slave device to the active device. The role flag strings (*3) and (*4) are added respectively to logs redirected from the two standby devices to the active device.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the log redirection function.

logging rd on

(4) (Optional) Configure the rate limit on redirected logs.

logging rd rate-limit *number* [**except** [*severity-level*]]

The log redirection function limits the maximum number of logs to be redirected per second to 200 by default.

1.10 Configuring Performance Logging Function

1.10.1 Overview

After the performance logging function is enabled, the logs that are output through the performance logging interface will be transmitted through the performance logging channel.

1.10.2 Restrictions and Guidelines

The performance logging function needs to be configured only when massive logs are displayed on the server within a short period. Only several functional services require this function.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the performance logging function.

logging performance switch

The performance logging function is disabled by default.

1.11 Configuring Synchronization of User Input and Log Output

1.11.1 Overview

When the synchronization of user input and log output is enabled, even if logs are displayed during user input, the user input information is displayed after display, thereby ensuring the input integrity and continuity.

1.11.2 Restrictions and Guidelines

The **logging synchronous** command is configured in line configuration mode, and on each line that enables this function.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Synchronize user input and log output.

logging synchronous

Synchronization of user input and log output is disabled by default.

1.12 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

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

Table 1-5 Syslog Monitoring

Command	Purpose
clear logging	Clears logs in the memory buffer.
show logging	Displays log statistics and logs in the memory buffer based on the timestamp from earliest to latest.

Command	Purpose
show logging reverse	Displays log statistics and logs in the memory buffer based on the timestamp from latest to earliest.
show logging config	Displays system log configurations and statistics.
show logging count	Displays log statistics of each module in the system.

1.13 Configuration Examples

1.13.1 Configuring the RFC5424 Log Format

1. Requirements

The network administrator can check system logs to learn about the operation status of the device, better understand and manage the device, or locate problems.

2. Topology

Figure 1-1 Topology for RFC5424 Log Format Configuration

3. Notes

- Configure the L3 network reachable between the device and the server.
- Enable logging
- Set the system log format to RFC5424 format.
- Configure log reporting.
  - Configure level-based log reporting.
  - Configure delayed log reporting.
  - Configure periodical log reporting.
- Configure log monitoring.
  - Configure the log statistics collection.
  - Set the rate of outputting system logs to the console to 50 logs per second.
  - Configure the display of logs on the monitor terminal.
- Synchronize user input and log output.
- Enable performance logging.
- Configure log filtering.
  - Set the filtering directions of logs to **terminal** and **server**.

- Set the log filtering mode to **filter-only**.
- Set the log filtering rule to **single-match** to filter the logs with a module name containing "SYS".

- Configure the output direction of system logs.
  - Configure the function of writing system logs into a log file named **syslog**.
  - Configure the transmission of system logs to the log server with the IPv4 address of 10.1.1.1.
  - Configure the size of the system logs to be written into the memory buffer to 128 KB (131072 bytes).

4. Procedure

(1) Configure the management IP address for the device.

```
Device> enable
Device# configure terminal
Device(config)#interface vlan 1
Device(config-if-VLAN 1)# ip address 10.1.1.2 255.255.255.0
Device(config-if-VLAN 1)# exit
```

(2) Enable logging

```
Device(config)# logging on
```

(3) Set the system log format to RFC5424 format.

```
Device(config)# service log-format rfc5424
```

(4) Configure log reporting.

Configure delayed log reporting.

```
Device(config)# logging delay-send terminal
Device(config)# logging delay-send interval 7200
Device(config)# logging delay-send file flash:syslog_ruijie
Device(config)# logging delay-send server 192.168.23.12 mode ftp user admin
password admin
```

Configure level-based log reporting.

```
Device(config)# logging policy module SYS not-lesser-than 5 direction console
Device(config)# logging policy module SYS 3 direction buffer
```

Configure periodical log reporting.

```
Device(config)# logging statistic enable
Device(config)# logging statistic terminal
Device(config)# logging statistic mnemonic TUNNEL_STAT interval 30
```

(5) Configure log monitoring.

```
Device(config)# logging userinfo
Device(config)# logging userinfo command-log
```

Configure log statistics collection.

```
Device(config)# logging count
```

Configure the output of system logs to the console.

```
Device(config)# logging console informational
```

Set the rate of outputting system logs to the console to 50 logs per second.

```
Device(config)# logging rate-limit console 50
```

Configure the output of system logs to the monitor terminal.

```
Device(config)# logging monitor informational
Device(config)# line vty 0 4
Device(config-line)# monitor
```

(6) Synchronize user input and log output

```
Device(config-line)# logging synchronous
Device(config-line)# exit
```

(7) Enable performance logging.

```
Device(config)# logging performance switch
```

(8) Configure system log filtering.

Set the filtering directions of logs to **terminal** and **server**.

```
Device(config)# logging filter direction server
Device(config)# logging filter direction terminal
```

Set the log filtering mode to **filter-only**.

```
Device(config)# logging filter type filter-only
```

Set the log filtering rule to **single-match** to filter the logs with a module name containing "SYS".

```
Device(config)# logging filter rule single-match module SYS
```

(9) Configure the output direction of system logs.

Configure the function of writing system logs into a log file named **syslog**.

```
Device(config)# logging file flash:syslog debugging
Device(config)# logging flash interval 600
```

Configure the transmission of system logs to the log server with the IPv4 address of 10.1.1.1.

```
Device(config)# logging server 10.1.1.1
```

Configure the size of the system logs to be written into the memory buffer to 128 KB (131072 bytes).

```
Device(config)# logging buffered 131072 informational
```

5. Verification

(1) Run the **ping** command to check whether the L3 route between the server and the log server is reachable.

```
Device# ping 10.1.1.1
Sending 5, 100-byte ICMP Echoes to 10.1.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms.
```

(2) Run the **show logging config** command to check the configuration result.

```
Device# show logging config
Syslog logging: enabled
  Console logging: level informational, 84 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level debugging, 92 messages logged
```

```
  File logging: level debugging, 105 messages logged
  File name:syslog.txt, size 128 Kbytes, the 1 file is currently being written
  Statistic log messages: enable
  Statistic log messages to terminal: enable
  Delay-send log messages to terminal: enable
  Delay-send file name:syslog_ruijie, Current write index:0, Current send index:0,
Cycle:7200 seconds
  Count log messages: enable
  Trap logging: level debugging, 84 message lines logged,10 fail
    logging to  10.1.1.100
  Delay-send logging: 0 message lines logged
    logging to  10.1.1.1  by ftp
```

6. Configuration Files

Device configuration file

```
hostname Device
!
service log-format rfc5424
logging filter direction server
logging filter direction terminal
logging filter rule single-match module SYS
logging rate-limit console 50
logging count
logging userinfo command-log
logging buffered 131072 informational
logging file flash:syslog debugging
logging flash interval 600
logging console informational
logging monitor informational
logging facility local7
logging server 10.1.1.1
logging performance switch
logging policy module SYS not-lesser-than 5 direction console
logging policy module SYS 3 direction buffer
logging statistic enable
logging statistic terminal
logging statistic mnemonic TUNNEL_STAT interval 30
logging delay-send terminal
logging delay-send interval 7200
logging delay-send file flash:syslog_ruijie
logging delay-send server 192.168.23.12 mode ftp user admin password admin
!
interface VLAN 1
 ip address 10.1.1.2 255.255.255.0
!
end
```

Contents

1 Configuring Software Upgrade....1
1.1 Introduction....1
1.2 Principles of System Version Upgrade....1
1.3 Principles of Patch Version Upgrade....3
1.3.1 Basic Concepts....3
1.3.2 Patch Package Management....3
1.3.3 Patch Auto-Sync....3
1.4 Configuration Task Summary....4
1.5 Configuring System Version Upgrade....4
1.5.1 Configuration Tasks....4
1.5.2 Configuring Subsystem Upgrade/Degrade....4
1.5.3 Configuring Version Auto-sync....5
1.6 Configuring Patch Version Upgrade....6
1.6.1 Overview....6
1.6.2 Configuration Tasks....6
1.6.3 Installing a Patch Package....6
1.6.4 Uninstalling a Patch Package....7
1.7 Monitoring....8
1.8 Configuration Examples....9
1.8.1 Configuring Subsystem Upgrade....9
1.8.2 Configuring Auto-sync Upgrade....11
1.8.3 Installing a Patch Package....12

1.8.4 Uninstalling a Patch Package 15

1 Configuring Software Upgrade

1.1 Introduction

Adopting a modular structure, Ruijie General Operating System (RGOS) supports overall system upgrade and subsystem upgrade, as well as the upgrade through patches. The package management module of RGOS is used to install, query, and maintain components of the device. By upgrading the software of the device, users can install software that is more stable or contains more features in the system.

1.2 Principles of System Version Upgrade

1. Basic Concepts

- Subsystem

  A subsystem exists on a device in the form of images. The RGOS subsystems include:

  - Uboot: After being powered on, the device loads and runs the Uboot subsystem. This subsystem initializes the device, and loads and runs system images.
  - Rboot: This subsystem is a set of dedicated programs used to install or upgrade the main program.
  - Basic Input Output System (BIOS): This subsystem is dedicated for devices running the X86 architecture.
  - Main program: This subsystem is a collection of Operating Systems (OSs) and applications in the system.

- Main package

  The main package is often used to upgrade/degrade subsystems of box-type devices. The main package is a combination package of the Uboot, Rboot, and main program subsystems. The main package is used for overall system upgrade/degradation.

- BIOS package

  The BIOS package is used to upgrade the BIOS of the device. It is used on the devices running the X86 architecture only.

Caution

An "installation package" in this document refers to installation files of all the subsystems of the device.

2. Upgrading/Degrading and Managing Subsystems

Subsystem upgrade/degradation aims to update the software functions by replacing the subsystem components in the device with the ones in an installation package. Redundancy design is adopted for subsystems, so subsystems of the device are often not directly replaced with the subsystems in the package during upgrade/degradation. Instead, subsystems are added to the device and then activated.

- Upgrade/Degradation

Subsystems exist on the device in different forms. Therefore, they are upgraded or degraded differently.

- Uboot: Generally, this subsystem exists in the NOR flash memory of the device in the form of images. It is upgraded/degraded by writing images into the NOR flash memory of the device.
- Rboot: Generally, this subsystem exists in the NOR flash memory of the device in the form of images. It is upgraded/degraded by writing images into the NOR flash memory of the device.
- BIOS: Generally, this subsystem exists in the flash memory of the device in the form of images. It is upgraded/degraded by writing images into the flash memory of the device.
- Main program: Generally, this subsystem exists in the NAND flash memory of the device in the form of images. It is upgraded/degraded by writing images into the NAND flash memory of the device.

- Management

  During upgrade of the subsystem component of the main program, the upgrade/degradation module always records the subsystem component in use, the redundant subsystem components, and management information of various versions in the configuration file. The module queries the available subsystem components and then loads subsystem components as needed.

  The redundancy design is adopted for each subsystem component. During the upgrade/degradation:

  - Uboot: This subsystem contains a master boot subsystem and a slave boot subsystem. Only the master boot subsystem is upgraded, and the slave boot subsystem is always redundant.
  - Rboot: This subsystem contains one program. More redundancies are allowed if there is enough space.
  - BIOS: This subsystem contains a master BIOS and a slave BIOS. The two BIOSs can be upgraded.
  - Main program: One redundancy is allowed if there is enough space.

- Upgrade

  Put upgrade files in the local device, and then run the **upgrade** command.

3. Auto-Sync Upgrade

Auto-sync upgrade aims to coordinate multiple subsystems (boards, chassis, and virtual switching unit (VSU) system) within one system. During software upgrade, the system automatically sends an upgrade package to all matched members, or upgrades the software version of new members to the specified version according to the specified upgrade policy to ensure that the software version of the entire system meets expectations.

- Select one from the following auto-sync upgrade policies:
  - Check the software version of a new member, and upgrade the member if its version is earlier than the version of the system installation package. Otherwise, no upgrade is performed.
  - Do not auto-sync new members.
  - Upgrade new members to the version of the system upgrade package regardless of the current version of the new members.
- Auto-sync upgrade check is performed in the following scenarios:
  - During upgrade, if no upgrade target is specified, the upgrade function module sends the upgrade package to all matched members (including boards, chassis, and VSU system) for auto-sync upgrade.
  - When the device is started, the version of every member is checked, and auto-sync upgrade is performed according to the version check result and auto-sync upgrade policy.
  - When a new member is added, the version of the member is checked and auto-sync upgrade is

performed according to the version check result and auto-sync upgrade policy.

- Management

  To perform auto-sync upgrade, configure an auto-sync upgrade policy and install an upgrade package.

- Configuring an auto-sync upgrade policy

  To perform the expected upgrade when a new member is added to the system, check the auto-sync upgrade configuration, such as preparation of the installation package.

  If a board is not checked because the system is not configured with an auto-sync upgrade policy, you can upgrade the specific members.

1.3 Principles of Patch Version Upgrade

1.3.1 Basic Concepts

- Patch package

  A patch package contains several patches. You can upgrade the package to fix various problems for the main program. If a patch package contains hot patches, they take effect before you restart the device restart. If a patch package contains cold patches, they take effect only after the device is restarted.

1.3.2 Patch Package Management

Upgrade of cold patches is to expand the component files in a package into the device. The upgrade takes effect only after the device is restarted.

Such process is similar to the upgrade of hot patches. But in the latter upgrade, only the files to be revised are replaced and then the new files take effect automatically.

Patch management is to use the database to record the patch information. The query, installation, and uninstallation correspond to the insertion, query, and deletion of the database.

Patch management includes three states: installed, activated, and confirmed:

- A patch in the installed state only indicates that this patch exists on the device, but it has not taken effect.
- Only a patch in the activated state is effective, but it will automatically roll back to the previous state after the device is restarted.
- A confirmed patch is also an effective patch, and the patch will not roll back even if the device is restarted.

1.3.3 Patch Auto-Sync

Patch auto-sync aims to coordinate multiple subsystems (boards and chassis) within a system. During software upgrade, the system automatically sends the patch installed on the current supervisor module to all the members meeting component installation rules. When a new member is added, the system automatically synchronizes the patch installed on the supervisor module to the new member. Thus, no resolved patch problem occurs even if synchronization is omitted.

Patch auto-sync rules:

- The subsystems comply with all the normal patch installation rules.
- The versions of all the subsystems must come from the same rack package before patch auto-sync is performed.
- The patch installed on the master supervisor module is used as the benchmark. If the same patch is

installed on a newly connected member but the patch status is higher than that of the current supervisor module, the patch on the new member is not be processed. The status order of patches is: add, active, and running.

1.4 Configuration Task Summary

Software upgrade configuration includes the following tasks:

- Configuring System Version Upgrade
  - a Configuring Subsystem Upgrade/Degrade
  - b (Optional) Configuring Version Auto-sync
- Configuring Patch Version Upgrade
  - a Installing a Patch Package
  - b Uninstalling a Patch Package

1.5 Configuring System Version Upgrade

1.5.1 Configuration Tasks

System version upgrade configuration includes the following tasks:

(1) Configuring Subsystem Upgrade/Degrade

(2) (Optional) Configuring Version Auto-sync

1.5.2 Configuring Subsystem Upgrade/Degrade

Warning

Boot upgrade is risky. If the device is powered off during upgrade, the device may be damaged and thus does not work. If the upgrade fails, do not power off the device, but attempt to upgrade the boot again.

1. Overview

Subsystem installation packages include the following types:

- Main package for device upgrade: After the upgrade using the main package is completed, all system software in the device is updated, and the overall software is enhanced.
- Rack package for upgrade: After the upgrade using the rack package is completed, all system software in the rack-type device is updated, and the overall software is enhanced.

Specification

Generally a main package is released to upgrade box-type devices.

2. Restrictions and Guidelines

- To upgrade a main package of the device, download the installation package to the local device and run the **upgrade** command.

- To upgrade a rack package, store the rack package in a USB flash drive or SD card of the device because the rack package is large, and then run the **upgrade** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Upgrade the installation package corresponding to the device.

upgrade [**boot**] { *url* | **download** { **oob_ftp**:*//path* [via mgmt { interface-number }] | **oob_tftp**:*//path* [**via mgmt** { *interface-number* }] | **ftp:***//path* [**vrf** *vrf-name*] | **tftp**:*//path* [**vrf** *vrf-name*] } [slot slot-number] } [**force**]

1.5.3 Configuring Version Auto-sync

1. Overview

This section describes how to configure a version auto-sync policy for a distributed system.

2. Restrictions and Guidelines

- To upgrade a new member in the system, check the version auto-sync upgrade configuration, such as preparation of the installation package.
- If a device member is not checked because the system is not configured with a version auto-sync policy, you can upgrade a specific member manually.
- After the path of an upgrade package used for version auto-sync is configured, the upgrade function module will determine the location of the installation package according to this path when new members (boards, chassis, or new VSU members) join the system. Each time the system is upgraded, the upgrade function module records the path of the installation package for this upgrade and uses it for version auto-sync. You can also use the **upgrade auto-sync package** command to set an upgrade package path.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure a version auto-sync policy.

upgrade auto-sync policy [**none** | **compatible** | **coordinate**]

Specification

All the parameters apply to only the VSUs.

(3) Configure the range of version auto-sync.

upgrade auto-sync range [**vsu**]

(4) Configure the path of the upgrade package for version auto-sync.

upgrade auto-sync package *url*

Specification

All the parameters apply to only the VSUs.

(5) Configure the status of the version auto-sync service.

upgrade sync-server [**close** | **open**]

1.6 Configuring Patch Version Upgrade

1.6.1 Overview

Besides the main program version, RGOS provides a patch mechanism to quickly fix the problems occurring on the main program version. A hot patch package can fix software bugs before the device is restarted; but an installed cold patch package can take effect only after the device is restarted. This patch package fixes a specific software version only. After the main program version is upgraded, the corresponding patch will become invalid automatically.

1.6.2 Configuration Tasks

Patch version configuration includes the following tasks:

(1) Installing a Patch Package

(2) Uninstalling a Patch Package

1.6.3 Installing a Patch Package

1. Overview

This section describes how to install a patch package to fix software bugs. A patch package is used to upgrade a specific version of software only.

2. Restrictions and Guidelines

- Before installing a patch package, download it to a local directory of the device.

Caution

The downloaded patch package cannot be renamed. The name of the patch package is used as the operation keyword for the subsequent patch activation, deactivation, and uninstallation.

- The installed patch must be activated before it is used. You must activate the patch first temporarily and then permanently. If a patch is activated temporarily, the patch will roll back to the previous state after the device is restarted. You can activate a patch temporarily only when verifying the patch function temporarily.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Download a patch package.

install add *url* [**slot** { **all** }]

(3) Install the patch package.

- Run the general patch command to install the patch package.

a Activate the installed patch temporarily.

install activate *package_name* [**slot** { **0** | **all** }]

b Activate the patch permanently.

install commit [**slot** { **0** | **all** }]

- Run the **patch** command to install the patch package.

---

a Activate the installed patch temporarily.

patch active [**slot** { **0** | **all** }]

b Activate the patch permanently.

patch running [**slot** { **0** | **all** }]

(4) Activate the patch permanently by one click.

patch auto-running [**slot** { **0** | **all** }]

1.6.4 Uninstalling a Patch Package

1. Overview

This section describes how to deactivate the activated patches and remove the existing patches from the device, that is, the database information.

2. Restrictions and Guidelines

For users, only one patch is effective on the device. Therefore, only one patch to be activated is allowed on the device. To install another patch package of a function component, you need to uninstall the previous patch.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Uninstall a patch.

- Run the general patch command to uninstall a patch package.

a Deactivate an activated patch.

install deactivate *package_name* [**slot** { **0** | **all** }]

b Uninstall a patch.

install remove *package_name* [**slot** { **0** | **all** }]

- Run the **patch** command to uninstall a patch package.

a Deactivate an activated patch.

patch deactivate *package_name* [**slot** { **0** | **all** }]

b Uninstall a patch.

patch delete [**slot** { **0** | **all** }]

1.7 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **check** commands to check information.

Run the **clear** commands to clear information.

Caution

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

Table 1-1 System Version Upgrade Monitoring

Command	Purpose
show upgrade status	Displays the upgrade status of the device and the installation status of a patch.
show upgrade history	Displays the upgrade history.
check version	Checks the version matching.

Table 1-2 Patch Version Upgrade Monitoring

Command	Purpose
install remove *package_name* [**slot** { **0** | **all** }]	Removes an unactivated patch package from a multi-patch solution.
patch delete [**slot** { **0** | **all** }]	Removes an unactivated patch package from a single-patch solution.
clear install storage [**slot** { 0| **all** }]	Clears all the patch packages not running currently and corresponding database information.
show install	Displays information about the hot patch package already installed on the device in a multi-patch solution.
show patch	Displays information about the hot patch package already installed on the device in a single-patch solution.
show install auto-sync	Displays whether the device enables patch auto-sync.

1.8 Configuration Examples

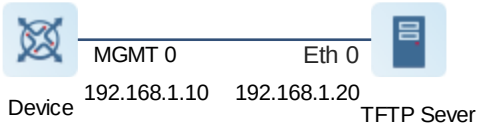
1.8.1 Configuring Subsystem Upgrade

1. Requirements

Upgrade a subsystem installation package to update all software in the device so that the overall software is enhanced and the known software bugs are fixed. Use Figure 1-1 as an example. The **upgrade download oob_tftp://***path* command is used to upgrade the subsystems of the device by using the installation package file stored on the TFTP server.

2. Topology

Figure 1-1 Subsystem Upgrade Topology



3. Notes

- Configure an IP address for the network management interface on the device so that the L3 route is reachable between the device and the TFTP server.
- Run the **upgrade download oob_tftp:**//*path* command to upgrade the installation package file stored on the TFTP server.

4. Procedure

(1) Configure an IP address for the network management interface on the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface mgmt 0
Hostname(config-if-Mgmt 0)# ip address 192.168.1.10 255.255.255.0
Hostname(config-if-Mgmt 0)# gateway 192.168.1.1
Hostname(config-if-Mgmt 0)# end
```

(2) Run the **upgrade download oob_tftp:**//*path* command to upgrade the device.

```
Hostname# upgrade download oob_tftp://192.168.1.20/main.bin via mgmt 0 force
*Nov 23 13:21:39: %UPGRADE-6-INFO: Copy to /tmp/vsd/0/upgrade_rep/
*Nov 23 13:21:39: %UPGRADE-6-INFO: Please wait for a moment......
Press Ctrl+C to quit
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!
< The terminal is locked by upgrade module >
Upgrade start
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!10%
< you can press Ctrl+C to unlock terminal >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!20%
< you can press Ctrl+C to unlock terminal >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!30%
< you can press Ctrl+C to unlock terminal >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!100%
Upgrade success
< The terminal is unlocked by upgrade module >
[Slot 0]
       Device type    : s6120
       Status        : success
```

(3) After upgrading the subsystems, run the **reload** command to restart the device so that the configuration takes effect.

```
Hostname# reload
Reload system?(Y/N)y
*Dec 25 06:48:02: %SYSMON-5-RELOAD: Reset system from [CONSOLE] with reason
[Management port/Reset system by reload command]
Hostname#*Dec 25 06:48:02: %DP-3-RESET_DEV: Reset device 1 due to
SYSMON/3766/CONSOLE/Management port/Reset system by reload command.
*Dec 25 06:48:04: %DP-3-MACHINE_RESTART: MACHINE_RESTART.
```

5. Verification

(1) Run the **ping** command to check whether the L3 route between the device and the TFTP server is reachable.

```
Hostname# ping oob 192.168.1.10
Sending 5, 100-byte ICMP Echoes to 192.168.1.20, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms.
```

(2) Run the **show upgrade status** command to display the upgrade result.

```
Hostname# show upgrade status
upgrade global status: INIT
[Slot 0]
       Device type    : s6120
       Status        : success
```

(3) Check the running version on the device. If the version information changes, the upgrade is successful.

```
Hostname# show version
System description     : Ruijie 10G Ethernet Switch(S6120-20XS4VS2QXS) By Ruijie
Networks
System start time      : 2020-11-23 13:13:59
System uptime         : 0:00:03:36
System hardware version : 1.0B
System software version : S6120_RGOS 12.1(PL1)
System patch number    : NA
```

```
System serial number    : 1234942570025
System boot version     : 1.4.2(Master) 1.4.2(Slave)
Module information:
  Slot 1/0 : RG-S6120-20XS4VS2QXS
    Hardware version    : 1.0B
    Boot version       : 1.4.2(Master) 1.4.2(Slave)
    Software version    : S6120_RGOS 12.1(PL1)
    Serial number      : 1234942570025
  Slot 2/0 : RG-S6120-20XS4VS2QXS
    Hardware version    : 1.00
    Boot version       : 1.4.2(Master) 1.4.2(Slave)
    Software version    : S6120_RGOS 12.1(PL1)
    Serial number      : 1234942570022
```

6. Common Errors

If an error occurs during the upgrade, the system displays the cause of the upgrade failure. You can also run the **show upgrade status** command to display the result of the last upgrade.

The following describes several types of common error messages:

- Invalid installation package: The possible cause is that the package is damaged or is not an installation package. You are advised to obtain the correct installation package and perform the upgrade again.
- Installation package not supported by the device: The possible cause is that you use the installation package of other devices. You are advised to obtain the correct installation package, verify the package information, and perform the upgrade again.
- Insufficient device space: Generally, this error occurs on a rack-type device. You are advised to check whether the device is equipped with a USB flash drive or SD card. Rack-type devices often have USB flash drives.

1.8.2 Configuring Auto-sync Upgrade

1. Requirements

On devices using a distributed structure such as rack-type devices and VSUs, auto-sync upgrade can upgrade the software version of matched members according to a configured auto-sync upgrade policy when software is upgraded or new members are added. This function ensures the coordination of the entire system. In the example of the VSU system using rack-type devices, we auto-sync an installation package.

2. Procedure

Configure an auto-sync upgrade policy based on the software version of the controlling device.

```
Hostname> enable
Hostname# upgrade auto-sync policy coordinate
```

Set the auto-sync upgrade range to the VSU system.

```
Hostname# upgrade auto-sync range vsu
```

3. Verification

Display the current auto-sync upgrade policy.

```
Hostname# show upgrade auto-sync
auto-sync range     : vsu
auto-sync policy    : coordinate
auto-sync package   : flash:install_file/S6120_install.bin
```

Check version matching of device nodes.

```
Hostname# check version
  Dev Slot State
  --- ---- ------------
  1   4    Compatible
  1   FE6  Compatible
  1   M1   Compatible
```

4. Common Errors

- The url parameter in the command used for configuring auto-sync upgrade does not point to a valid upgrade package.

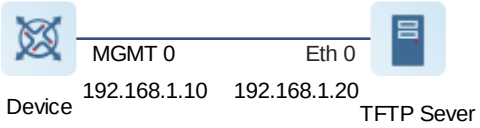
1.8.3 Installing a Patch Package

1. Requirements

Install a patch package to fix software bugs without upgrading the main program version.

2. Topology

Figure 1-2 Patch Package Installation Topology



3. Notes

(1) Configure the L3 route reachable to the device.

(2) Copy the patch package to the device.

(3) Run the patch installation command.

(4) Activate a hot patch.

a Activate a hot patch temporarily.

b Activate a hot patch permanently.

(5) Configure patch auto-sync.

4. Procedure

(1) Configure an IP address for the network management interface on the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#interface mgmt 0
Hostname(config-if-Mgmt 0)# ip address 192.168.1.10 255.255.255.0
```

```
Hostname(config-if-Mgmt 0)# gateway 192.168.1.1
```

(2) Install a patch package.

```
Hostname# install add tftp//192.1.1.20/smu_rf_hot1002_0118.bin
< The terminal is locked by patch moduleed by patch module >
Press Ctrl+C to quit
!
Operating, please wait for a moment.....
Operate finish!
Operate result information:
-------------------------------------
Slot          Result        Comment
1/0           Success       None
2/0           Success       None

< The terminal is unlocked by patch module >
```

(3) Activate a patch.

- Run the **install** command to activate the patch.

  a Run the **install active** command to activate the hot patch temporarily.

```
Hostname# install activate smu_rf_hot1002_0118.bin
< The terminal is locked by patch module >
Operating, please wait for a moment.......
Operate finish!
Operate result information:
-------------------------------------
1/0           Success       None
2/0           Success       None

< The terminal is unlocked by patch module >
```

  b Run the **install commit** command to activate the hot patch permanently.

```
Hostname# install commit
< The terminal is locked by patch module >
Operating, please wait for a moment...
Operate finish!
Operate result information:
-------------------------------------
Slot          Result        Comment
1/0           Success       None
2/0           Success       None

< The terminal is unlocked by patch module >
Hostname#
```

- Run the **patch** command to activate the patch.

  a Run the **patch active** command to activate the hot patch temporarily.

```
Hostname# patch active
< The terminal is locked by patch module >
Operating, please wait for a moment.......
Operate finish!
Operate result information:
-------------------------------------
1/0          Success       None
2/0          Success       None

< The terminal is unlocked by patch module >
```

b Run the **patch running** command to activate the hot patch permanently.

```
Hostname# patch running
< The terminal is locked by patch module >
Operating, please wait for a moment...
Operate finish!
Operate result information:
-------------------------------------
Slot         Result        Comment
1/0          Success       None
2/0          Success       None

< The terminal is unlocked by patch module >
```

(4) Configure patch auto-sync.

```
Hostname# install sync enable
```

5. Verification

(1) Display the patch installation information.

Run the **show install** command to display information about the hot patch installed on the current device.

```
Hostname# show install
Install information:
 [Slot 1/0]
    Name                 Package         State         Flag       Effective time
    smu_rf_hot1002_0118.bin               Running       Hot        2019-09-17
19:00:02

 [Slot 2/0]
    Name                 Package         State         Flag       Effective time
    smu_rf_hot1002_0118.bin               Running       Hot        2019-09-17
19:00:02
```

Run the **show patch** command to display information about the hot patch installed on the current device.

```
Hostname# show patch
 [Slot 1/0]
    Patch name         : smu_rf_hot1002_0118
    File name          : smu_rf_hot1002_0118.bin
```

```
    Patch state        : Install
    Patch flag         : Hot
    Effective time      :
    Last patch         :

 [Slot 2/0]
    Patch name         : smu_rf_hot1002_0118
    File name          : smu_rf_hot1002_0118.bin
    Patch state        : Install
    Patch flag         : Hot
    Effective time      :
    Last patch         :
```

6. Common Errors

- If you run the **install commit** command when a patch is not activated, an error is prompted. The **install commit** command takes effect only when the patch is in the active state.
- If you run the **patch running** command when a patch is not activated, an error is prompted. The **patch running** command takes effect only when the patch is in the active state.

1.8.4 Uninstalling a Patch Package

1. Requirements

One function component in one device can run one patch only. To install a new patch for this function component, you need to uninstall the previous patch before installation.

2. Notes

(1) Run the patch deactivation command.

(2) Run the patch uninstall command.

3. Procedure

(1) Uninstall a patch.

- Run the **install** command to uninstall a patch.

  a Run the **install deactivate** command to deactivate the patch.

```
Hostname# install deactivate smu_rf_hot1002_0118.bin
< The terminal is locked by patch module >
Operating, please wait for a moment.......
Operate finish!
Operate result information:
-------------------------------------
1/0          Success       None
2/0          Success       None

< The terminal is unlocked by patch module >
```

  b Run the **install remove** command to uninstall the patch.

```
Hostname#install remove smu_rf_hot1002_0118.bin
```

```
< The terminal is locked by patch module >
Operating, please wait for a moment...
Operate finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None

< The terminal is unlocked by patch module >
```

- Run the **patch** command to uninstall a patch.

  a Run the **patch deactive** command to deactivate the patch.

```
Hostname# patch deactive
< The terminal is locked by patch module >
Operating, please wait for a moment.......
Operate finish!
Operate result information:
-------------------------------------
1/0          Success      None
2/0          Success      None

< The terminal is unlocked by patch module >
```

  b Run the **patch delete** command to uninstall the patch.

```
Hostname# patch delete
< The terminal is locked by patch module >
Operating, please wait for a moment...
Operate finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None

< The terminal is unlocked by patch module >
```

4. Verification

(1) Display the patch status.

Run the **show install** command to display the patch uninstallation result.

```
Hostname#show install
[Slot 1/0]
    [No Install information]

 [Slot 2/0]
    [No Install information]
```

Run the **show patch** command to display the patch uninstallation result.

```
Hostname# show patch
 [Slot 1/0]
    [No Install information]

 [Slot 2/0]
    [No Install information]
```

Contents

1 Configuring Uboot 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Accessing the Uboot Menu 1
1.1.3 Downloading XModem 2
1.1.4 Running the Main Program 2
1.1.5 Running the Rboot Program 2
1.1.6 Querying and Setting Other Functions 2
2 Configuring the SIMPLE CLI 4
2.1 Introduction 4
2.1.1 Overview 4
2.1.2 Accessing the SIMPLE CLI Operation Interface 4
2.1.3 Downloading Xmdown 5
2.1.4 Running the Rboot Program 5
2.1.5 Running the Main Program 5
2.1.6 Setting the Baud Rate 6
2.1.7 Reloading the System 6
2.1.8 Displaying the Version 6
2.1.9 Skipping to the Menu Interface 6

1 Configuring Uboot

1.1 Introduction

1.1.1 Overview

The Uboot menu includes all functions supported by the universal boot loader (Uboot), including booting the main program, booting Rboot, and updating Uboot or Rboot.

1.1.2 Accessing the Uboot Menu

1. Connecting to the Client

Connect the COM port of a PC to the serial port of the device through a serial port cable, start the HyperTerminal, and configure the following settings:

- Protocol type for connection: Serial
- Port for connection: COM
- Bits per second: 9600
- Data bit: 8
- Parity check: N/A
- Stop bit: 1
- Data flow control: N/A

2. Starting the Device

After the device is started, the following information is displayed:

```
Press Ctrl+B to enter Boot Menu, Press Ctrl+C to enter Rboot
```

Press **Ctrl+B**.

3. Accessing the Uboot Menu Interface

The interface is displayed as follows:

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
   TOP menu items.
***********************************************
   0. XModem utilities.
   1. Run main.
   2. Run rboot.
   3. Scattered utilities.
***********************************************
Press a key to run the command:
```

After the device displays the menu interface, select a menu item to select the corresponding function.

Press the first character of the menu item to perform the function of the menu item. If the menu item is a submenu, the submenu is accessed. The device displays the interface of the submenu.

Press **Ctrl+Z** to exit the current submenu and return to the previous-level menu.

1.1.3 Downloading XModem

On the menu interface, select **Upgrade bootloader**.

This is a submenu. After you access the submenu, the following information is displayed:

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
   XModem utilities.
************************************************
   0. Upgrade bootloader.
   1. Upgrade rboot.
************************************************
Press a key to run the command:
```

1. Upgrading bootloader

This function downloads a Uboot file to the flash memory to update the master Uboot of the system.

(1) On the menu interface, select **Upgrade bootloader**.

(2) Click **Send File** under **Transfer** in HyperTerminal and select a Uboot image file to be downloaded (for example, **UBOOT.BIN**).

(3) Click **Send**.

(4) Wait until the system displays a message indicating that the operation is complete.

2. Upgrading rboot

This function downloads an Rboot file to the flash memory to update Rboot of the system.

(1) On the menu interface, select **Upgrade rboot**.

(2) Click **Send File** under **Transfer** in HyperTerminal and select an Rboot image file to be downloaded (for example, **RBOOT.BIN**).

(3) Click **Send**.

(4) Wait until the system displays a message indicating that the operation is complete.

1.1.4 Running the Main Program

On the menu interface, select **Run main**. The program automatically skips to the main program from Uboot.

1.1.5 Running the Rboot Program

On the menu interface, select **Run rboot**. The program automatically skips to Rboot from Uboot.

1.1.6 Querying and Setting Other Functions

On the menu interface, select **Scattered utilities**.

This is a submenu. After you access the submenu, the following information is displayed:

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
   Scattered utilities.
************************************************
   0. Show the bootloader version.
```

```
   1. Reload system.
   2. Set baudrate.
   3. Set default environment.
   4. Set debug mode.
5. Run main without enable password.
************************************************
Press a key to run the command:
```

1. Showing the bootloader Version

This function is used to display the version of the boot program on the current flash memory.

(1) On the menu interface, select **Show the bootloader version**.

(2) The version of Uboot is displayed.

Information similar to the following is displayed:

```
'master_bootloader' program information:
 Version:     1.3.13
'slave_bootloader' program information:
 Version:     1.3.13
```

2. Reloading the System

On the menu interface, select **Reload system**. The system reboots automatically.

3. Setting the Baudrate

This is a submenu. In the submenu, select **Set baudrate**. The following information is displayed:

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
   Set baudrate.
************************************************
   0. Change baudrate to 9600
   1. Change baudrate to 57600
   2. Change baudrate to 115200
************************************************
Press a key to run the command:
```

- On the menu interface, select **Change baudrate to 9600**. The system changes the baud rate to **9600**.
- On the menu interface, select **Change baudrate to 57600**. The system changes the baud rate to **57600**.
- On the menu interface, select **Change baudrate to 115200**. The system changes the baud rate to **115200**.

4. Setting the Default Environmental Variable

This function is used to replace the environmental variable stored on the flash memory with the default environmental variable.

On the menu interface, select **Set default environment**. The following information is displayed:

```
Warning: The environment information maybe lose, Are you sure to continue? [yes/No]:
```

Enter **yes** or **no**. If you do not enter any character, **no** is used by default. When this menu is used to set the default environmental variable, the baud rate is not restored to the default value. The baud rate currently saved on the flash memory is still used.

5. Setting the Debugging Mode

This is a submenu. After you access the submenu, the following information is displayed:

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
   Set debug mode.
************************************************
   0. Debug switch On.
   1. Debug switch Off.
************************************************
Press a key to run the command:
```

Select **Debug switch On** to enable the debugging mode or select **Debug switch Off** to disable the debugging mode.

The main program and Rboot output more boot logs in debugging mode than those in normal mode.

6. Starting the Main Program without Enabling Password

On the menu interface, select **Run main without enable password**. Click **OK**. The main program is started. In the main program, you can enable the device without a password. This function is used when you forget the password. This function is effective for only the current operation. After reboot, the password is still required.

2 Configuring the SIMPLE CLI

2.1 Introduction

2.1.1 Overview

The SIMPLE command line interface (CLI) includes some functions supported by Uboot, which are implemented through command lines, including booting the main program, booting Rboot, and updating Uboot or Rboot.

2.1.2 Accessing the SIMPLE CLI Operation Interface

On the Uboot menu interface, press **Ctrl+Q** to access the SIMPLE CLI operation interface.

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
   TOP menu items.
************************************************
   0. XModem utilities.
   1. Run main.
   2. Run rboot.
   3. Scattered utilities.
************************************************
Press a key to run the command:
```

Enter **help**. The functions of commands are displayed as follows:

```
bootloader# help
Total commands:
```

```
help           Dump command list OR show a command's details
xmdown          Download programs through XModem.
runrboot        Run rboot program.
runmain         Run main program.
setbaud         Set BOOT/BOOTLOADER baudrate tools.
reload          Reload tools.
version         Show current version information.
quit           Quit from CLI command line.
```

2.1.3 Downloading Xmdown

You can run this command to upgrade the main Uboot program and Rboot program on the flash memory.

Enter **help xmdown**. The usage details of the **xmdown** command are displayed.

```
bootloader# help xmdown
Syntax: xmdown (-boot | -rboot)
Usage Details:
   -boot:     Upgrade BootLoader.
   -rboot:  Upgrade Rboot.
Examples:
   xmdown -boot
   xmdown -rboot
```

1. xmdown -boot

This command is used to upgrade the main Uboot program on the flash memory.

(1) Enter **xmdown –boot** and press **Enter**.

(2) Click **Send File** under **Transfer** in HyperTerminal and select a Uboot image file to be downloaded (for example, **UBOOT.BIN**).

(3) Click **Send**.

(4) Wait until the system displays a message indicating that the operation is complete.

2. xmdown -rboot

This command is used to upgrade the Rboot program on the flash memory.

(1) Enter **xmdown –rboot** and press **Enter**.

(2) Click **Send File** under **Transfer** in HyperTerminal and select an Rboot image file to be downloaded (for example, **RBOOT.BIN**).

(3) Click **Send**.

(4) Wait until the system displays a message indicating that the operation is complete.

2.1.4 Running the Rboot Program

Enter the **runrboot** command. The program automatically skips to Rboot from Uboot.

2.1.5 Running the Main Program

Enter the **runmain** command. The program automatically skips to the main program from Uboot.

2.1.6 Setting the Baud Rate

After the **setbaud** command is run, the baud rate of the current device is changed and the changed baud rate is saved to the environmental variable partition of the flash memory.

Enter the **help setbaud** command. The usage details of the **setbaud** command are displayed:

```
ruijie#help setbaud
Syntax: setbaud (-h | -m | -l)
Usage Details:
   -h:        Set to 115200
   -m:        Set to 57600
   -l:        Set to 9600
Examples:
   setbaud -l
   setbaud -m
setbaud -h
```

- setbaud -l: The baud rate of the current device is changed into **9600** and the changed baud rate is saved to the environmental variable partition of the flash memory.
- setbaud -m: The baud rate of the current device is changed into **57600** and the changed baud rate is saved to the environmental variable partition of the flash memory.
- setbaud -h: The baud rate of the current device is changed into **115200** and the changed baud rate is saved to the environmental variable partition of the flash memory.

2.1.7 Reloading the System

Enter the **reload** command and press **Enter**. The system reboots automatically.

2.1.8 Displaying the Version

Enter the **version** command and press **Enter**. The system displays the versions of the master Uboot and slave Uboot. For example:

```
bootloader# version
'master_bootloader' program information:
  Version:     1.3.13
'slave_bootloader' program information:
  Version:     1.3.13
```

2.1.9 Skipping to the Menu Interface

Enter the **quit** command and press **Enter**. The system returns to the menu interface.

Contents

1 Configuring Rboot 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Accessing the Rboot Menu 1

1.1.3 Downloading Tftp utilities 2

1.1.4 Downloading X/Y/ZModem 3

1.1.5 Running the Main Program 6

1.1.6 Querying and Setting Other Functions 6

1 Configuring Rboot

1.1 Introduction

1.1.1 Overview

The Rboot menu includes all functions supported by Rboot, including booting the main program, updating the universal boot loader (Uboot), updating Rboot, and reinstalling the system.

1.1.2 Accessing the Rboot Menu

1. Connecting to the Client

Connect the COM port of a PC to the serial port of the device through a serial port cable, start the client software, and configure the following settings:

- Protocol type -for connection: Serial
- Port for connection: COM
- Bits per second: 9600
- Data bit: 8
- Parity check: N/A
- Stop bit: 1
- Data flow control: N/A

2. Starting the Device

After the device is started, the following information is displayed:

```
Press Ctrl+B to enter Boot Menu, Press Ctrl+C to enter Rboot
```

Press **Ctrl+C**.

When Rboot is started, the current version is displayed.

```
Rboot                        Version: 1.1.22
-----------------------------------------------
```

3. Accessing the Rboot Menu Interface

The interface displays the following:

```
====== Rboot Menu(Ctrl+Z to upper level) ======
   TOP menu items.
***********************************************
   0. Tftp utilities.
   1. X/Y/ZModem utilities.
   2. Run main.
   3. SetMac utilities.
   4. Scattered utilities.
```

```
************************************************
Press a key to run the command:
```

After the device displays the menu interface, select a menu item to select the corresponding function.

Press the first character of the menu item to perform the function of the menu item. If the menu item is a submenu, the submenu is accessed. The device displays the interface of the submenu.

Press **Ctrl+Z** to exit the current submenu and return to the previous-level menu.

1.1.3 Downloading Tftp utilities

This is a submenu. After you access the submenu, the following information is displayed:

```
====== Rboot Menu(Ctrl+Z to upper level) ======
   Tftp utilities.
************************************************
   0. Upgrade uboot/bios program.
   1. Upgrade rboot program.
   2. Upgrade main program.
   3. Upgrade the entire device by distribute package.
   4. Burn the total FlashROM by this downloaded file.
************************************************
Press a key to run the command:
```

1. Upgrading Uboot/Bios

This function downloads a Uboot or BIOS file to the flash memory to update the master or slave Uboot of the system or the master or slave BIOS of the system, depending on the product.

(1) Start the Trivial File Transfer Protocol (TFTP) server on the PC or supervisor module.

(2) Be sure to put the Uboot or BIOS upgrade image file to be downloaded in the TFTP server directory of the PC or supervisor module.

(3) Connect the device to the PC through an Ethernet cable.

(4) On the menu interface, select **Upgrade uboot/bios program**.

(5) Enter **Local IP** (IP address of the switch), **Remote IP** (IP address of the PC), and **Filename** (name of the Uboot or BIOS file to be downloaded) based on prompts and press **Enter**.

(6) Wait until the system displays a message indicating that the operation is complete.

2. Upgrading Rboot

This function downloads an Rboot file to the flash memory to update Rboot of the system.

(1) Start the TFTP server on the PC or supervisor module.

(2) Be sure to put the Rboot upgrade image file to be downloaded in the TFTP server directory of the PC or supervisor module.

(3) Connect the device to the PC through an Ethernet cable.

(4) On the menu interface, select **Upgrade rboot program**.

(5) Enter **Local IP** (IP address of the switch), **Remote IP** (IP address of the PC), and **Filename** (name of the Rboot file to be downloaded) based on prompts and press **Enter**.

3. Upgrading the Main Program

The function is used to parse a main program package and upgrade the main program. If the main program package contains Uboot or Rboot, Uboot or Rboot is upgraded depending on the version.

(1) Start the TFTP server on the PC or supervisor module.

(2) Be sure to put the upgrade image file of the main program to be downloaded in the TFTP server directory of the PC or supervisor module.

(3) Connect the device to the PC through an Ethernet cable.

(4) On the menu interface, select **Upgrade main program**.

(5) Enter **Local IP** (IP address of the switch), **Remote IP** (IP address of the PC), and **Filename** (name of the main program file to be downloaded) based on prompts and press **Enter**.

(6) Wait until the system displays a message indicating that the operation is complete.

4. Upgrade the Software Package

This function is used to parse a software package, retrieve the main program from the software package, and upgrade the device by using the main program according to the upgrade procedure of the main program.

(1) Start the TFTP server on the PC or supervisor module.

(2) Be sure to put the upgrade image file of the software package to be downloaded in the TFTP server directory of the PC or supervisor module.

(3) Connect the device to the PC through an Ethernet cable.

(4) On the menu interface, select **Upgrade the entire device by distribute package**.

(5) Enter **Local IP** (IP address of the switch), **Remote IP** (IP address of the PC), and **Filename** (name of the program file to be downloaded) based on prompts and press **Enter**.

(6) Wait until the system displays a message indicating that the operation is complete.

5. Upgrading the Flash ROM File

This function is used to refresh the ROM files (including the slave Uboot, master Uboot, and Rboot) in the flash memory to burn such files into the flash memory again. After upgrade, the baud rate is changed to **9600** and **SetMac** needs to be set again.

(1) Start the TFTP server on the PC or supervisor module.

(2) Be sure to put the ROM upgrade image file to be downloaded in the TFTP server directory of the PC or supervisor module.

(3) Connect the device to the PC through an Ethernet cable.

(4) On the menu interface, select **Burn the total FlashROM by this downloaded file**.

(5) Enter **Local IP** (IP address of the switch), **Remote IP** (IP address of the PC), and **Filename** (name of the program file to be downloaded) based on prompts and press **Enter**.

(6) Wait until the system displays a message indicating that the operation is complete.

1.1.4 Downloading X/Y/ZModem

This is a submenu. After you access the submenu, the following information is displayed:

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
```

```
   XModem utilities.
************************************************
   X/Y/ZModem utilities.
************************************************
   0. XModem utilities.
   1. YModem utilities.
   2. ZModem utilities.
   3. Local utilities.
************************************************
Press a key to run the command:
```

1. Upgrading XModem

This function is used to download Uboot, BIOS, Rboot, main program, software package, or ROM through XMODEM and install it on the device.

(1) On the menu interface, select **XModem utilities**.

(2) The device displays the following submenus:

```
====== Rboot Menu (Ctrl+Z to upper level) ======
   XModem utilities.
************************************************
   0. Upgrade uboot/bios program.
   1. Upgrade rboot program.
   2. Upgrade main program.
   3. Upgrade the entire device by distribute package.
   4. Burn the total FlashROM by this downloaded file.
************************************************
Press a key to run the command:
```

(3) Select a required upgrade type.

(4) Select **Transfer** > **Send File** in HyperTerminal, select **XMODEM** for the protocol, and select a file to be downloaded by the upgrade type.

(5) Click **Send**.

(6) Wait until the system displays a message indicating that the operation is complete.

2. Upgrading YModem

This function is used to download Uboot, BIOS, Rboot, main program, software package, or ROM through YMODEM and install it on the device.

(1) On the menu interface, select **YModem utilities**.

(2) The device displays the following submenus:

```
====== Rboot Menu (Ctrl+Z to upper level) ======
   YModem utilities.
************************************************
   0. Upgrade uboot/bios program.
   1. Upgrade rboot program.
   2. Upgrade main program.
```

```
   3. Upgrade the entire device by distribute package.
   4. Burn the total FlashROM by this downloaded file.
************************************************
Press a key to run the command:
```

(3) Select a required upgrade type.

Note

This menu is similar to the TFTP menu. For details, see the TFTP menu.

(4) Select **Transfer** > **Send File** in HyperTerminal, select **YMODEM** for the protocol, and select a file to be downloaded by upgrade type.

(5) Click **Send**.

(6) Wait until the system displays a message indicating that the operation is complete.

3. Upgrading ZModem

This function is used to download Uboot, BIOS, Rboot, main program, software package, or ROM through ZMODEM and install them on the device.

(1) On the menu interface, select **ZModem utilities**.

(2) The device displays the following submenus:

```
====== Rboot Menu (Ctrl+Z to upper level) ======
   ZModem utilities.
************************************************
   0. Upgrade uboot/bios program.
   1. Upgrade rboot program.
   2. Upgrade main program.
   3. Upgrade the entire device by distribute package.
   4. Burn the total FlashROM by this downloaded file.
************************************************
Press a key to run the command:
```

(3) Select a required upgrade type.

(4) Select **Transfer** > **Send File** in HyperTerminal, select **ZMODEM** for the protocol, and select a file to be downloaded by upgrade type.

(5) Click **Send**.

(6) Wait until the system displays a message indicating that the operation is complete.

4. Upgrading Local Utilities

This function is used to download the Uboot, BIOS, Rboot, main program, software package, and ROM to a USB flash drive or flash memory partition and install them on the device.

(1) On the menu interface, select **Local utilities**.

(2) The device displays the following submenus:

```
====== Rboot Menu (Ctrl+Z to upper level) ======
   Local utilities.
```

```
************************************************
   0. Upgrade uboot/bios program.
   1. Upgrade rboot program.
   2. Upgrade main program.
   3. Upgrade the entire device by distribute package.
   4. Burn the total FlashROM by this downloaded file.
************************************************
Press a key to run the command:
```

(3) Select a required upgrade type.

(4) Based on the prompt, enter a file path.

a If a USB flash drive is used, the file path is the location of the **usb0:** file. If there are multiple USB flash drives or partitions, the file paths are usb1: file location, usb2: file location, and so on.

b If a flash memory partition is used, the file path is the location of the **flash:** file.

(5) Wait until the system displays a message indicating that the operation is complete.

1.1.5 Running the Main Program

On the menu interface, enter **3**. The program is booted to access the main program.

1.1.6 Querying and Setting Other Functions

This is a submenu. After you access the submenu, the following information is displayed:

```
====== Rboot Menu(Ctrl+Z to upper level) ======
   Scattered utilities.
************************************************
   0. Show Version.
   1. Reload System.
   2. Set Baudrate.
   3. Format Flash.
   4. Exit menu.
   5. Set debug mode.
   6. Run main without enable password.
   7. Set Download Gateway.
************************************************
Press a key to run the command:
```

Note

Options in the submenu increases with the update of the Rboot version but some Rboot items of some earlier products may not be listed.

1. Displaying the Boot Version

This function is used to display the versions of Uboot/BIOS and Rboot on all flash memories.

(1) On the menu interface, select **Show Version**.

(2) The system displays versions of Uboot/BIOS and Rboot.

Example:

```
The First  MasterBoot Version: 1.3.13
The First  SlaveBoot  Version: 1.3.13
The First  Rboot     Version: 1.0.5
The Second MasterBoot Version: 1.3.13
The Second SlaveBoot  Version: 1.3.13
The Second Rboot     Version: 1.0.5
```

Note

Some devices may not display all the six boot programs above and NA is displayed for the inexistent boot programs.

2. Reloading the System

On the menu interface, select **Reload System**. The system reboots automatically.

3. Setting the Baud Rate

This is a submenu. After you access the submenu, the following information is displayed:

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
   Set baudrate.
************************************************
   0. Change baudrate to 9600
   1. Change baudrate to 57600
   2. Change baudrate to 115200
************************************************
Press a key to run the command:
```

- On the menu interface, select **Change baudrate to 9600**. The system changes the baud rate to **9600**.
- On the menu interface, select **Change baudrate to 57600**. The system changes the baud rate to **57600**.
- On the menu interface, select **Change baudrate to 115200**. The system changes the baud rate to **115200**.

Note

The configuration applies to the boot program. In the main program, the baud rate of the boot program may change with the configuration of the main program.

4. Formatting the Main Storage Partition

Warning

If this function is used, the main program and all configurations of the device and all files in the flash memory partition are lost. Therefore, do not use this function unless necessary.

On the menu interface, select **Format Flash**. The main partition is formatted and a partition table is recreated.

5. Setting the Debugging Mode

This is a submenu. After you access the submenu, the following information is displayed:

```
====== Rboot Menu (Ctrl+Z to upper level) ======
   Set debug mode.
***********************************************
   0. Debug switch On.
   1. Debug switch Off.
***********************************************
Press a key to run the command:
```

Select **Debug switch On** to enable the debugging mode or select **Debug switch Off** to disable the debugging mode.

The main program outputs more logs in debugging mode than those in normal mode.

6. Running the Main Program Without Enabling Password

On the menu interface, select **Run main without enable password**. Click **OK**. The main program is started. In the main program, you can enable the device without a password. This function is used when you forget the password. This function is effective for only the current operation. After reboot, the password is still required.

Some devices do not support startup without a password under Rboot (but supports startup without a password under Uboot). In this case, the following information is displayed:

```
   Not supported in Rboot.
   Please reload, press Ctrl+B to enter Uboot,
   and select the same item in Uboot menu.
```

For such devices, access Uboot during startup and select the **Run main without enable password** menu.

7. Downloading TFTP Across Gateways

This function is used to configure a gateway and a mask so that TFTP can be downloaded across gateways.

On the menu interface, select **Set Download Gateway**. The following information is displayed:

```
Plz enter the Local GatewayIP [<NULL>]:
```

Enter the IP address of a gateway in the format of X.Y.Z.W. The following message is displayed:

```
Plz enter the IP Netmask [<NULL>]:
```

Enter a subnet mask in the format of X.Y.Z.W. The following message is displayed:

```
   Set Local GatewayIP to <set IP address of the gateway>
Set IP Netmask to <set subnet mask>
```

Then return to the main menu and select items in **Tftp utilities**. The gateway and subnet mask are displayed during downloading and TFTP items are downloaded across gateways.

```
   TFTP: Detect Gateway <set IP address of the gateway> ...
   TFTP: Detect Netmask <set subnet mask> ...
```

The gateway configuration is not retained. After you leave Rboot, the configuration is lost.

To clear the gateway configuration in Rboot, enter a null address in **Set Download Gateway**.

```
Plz enter the Local GatewayIP [<NULL>]:
Plz enter the IP Netmask [<NULL>]:
```

```
Clear Local GatewayIP config.
Clear IP Netmask config.
```

Contents

1 Configuring Time Range 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Configuring Basic Features 1
1.2.1 Overview 1
1.2.2 Restrictions and Guidelines 1
1.2.3 Procedure 2
1.3 Monitoring 2
1.4 Configuration Examples 2
1.4.1 Configuring Basic Features of Time Range 2

1 Configuring Time Range

1.1 Introduction

1.1.1 Overview

Time range is a time control service. Users can create a time range and reference the time range in a service to control the time of the service. For example, to make an access control list (ACL) take effect in a time range within a week, configure a time range and associate the ACL with the time range. In this case, the ACL is effective only in the specified time range.

1.1.2 Principles

1. Basic Concepts

A time range is defined in the following modes:

- Absolute time range

  An absolute time range indicates the time range from the specified start time to the end time, for example, from 12:00:00 on January 1, 2000 to 12:00:00 on January 1, 2001.

- Period

  A period indicates a periodic time range, for example, from 8:00 Monday to 17:00 Friday.

2. Using an Absolute Time Range

When a function is enabled in a service that references a time range, the service determines whether the current time of the system is in an absolute time range. If yes, the function can be enabled or disabled in the current time.

3. Using a Period

When a function is enabled in an application based on a time range, the application determines whether the current time of the system is in a period. If yes, the function can be enabled or disabled in the current time.

1.2 Configuring Basic Features

1.2.1 Overview

This section describes how to create a time range and configure an absolute time range or a period.

1.2.2 Restrictions and Guidelines

- Before modifying an absolute time range or a period for a service, you are advised to disassociate the time range. After the absolute time range or period is modified, associate the time range again.
- In a time range, you can configure multiple effective periods.
- If an absolute time range and a period are configured in a time range, the effective time range is a period in the absolute time range. If multiple periods are configured, the effective time is the multiple periods configured in the absolute time range.

1.2.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a time range.

time-range *time-range-name*

(4) (Optional) Configure effective time of the time range. Configure at least one of the following tasks.

- Configure an absolute time range.

  absolute { **start** *hh:mm DD/MM/YY* | **end** *hh:mm DD/MM/YY* }*

  No absolute time range is configured. The maximum time range is used by default.

- Configure a period.

  periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*

  No period is configured by default. The current time is considered to be within a period.

1.3 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Time Range Monitoring

Command	Purpose
show time-range [*time-range-name*]	Displays a time range.

1.4 Configuration Examples

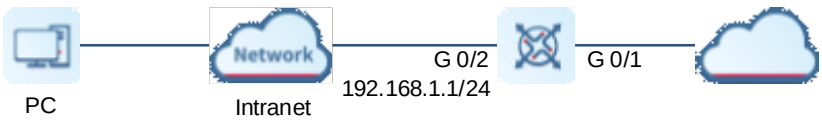
1.4.1 Configuring Basic Features of Time Range

1. Requirements

In the traffic control, an enterprise needs to control the traffic type and traffic in a specific period. For example, an enterprise prohibits employees from accessing the Internet during work and allows them to do so after work. In this case, an ACL can be configured to associate with a time range. During the working hours (9:00 to 12:00 and 14:00 to 18:00), PCs in the Intranet are prohibited from accessing the Internet. In other time ranges, the PCs are allowed to access the Internet. The PCs can access one another at any time.

2. Topology

Figure 1-1 Topology for Configuring the Basic Features of Time Range



3. Notes

- First configure system time for the device. The effective time of an ACL is based on the system time of the device.
- A time range cannot cross 0:00, that is, to create a time range from 22:00 to 7:00 the next day, create two time ranges.

4. Procedure

Configure system time in the following format: hh:mm:ss MMDDYY.

```
Hostname> enable
Hostname # clock set 10:00:00 12 1 2012
```

Set the time zone of the device to GMT+8.

```
Hostname# configure terminal
Hostname(config)# clock timezone beijing 8
```

Create a time range named **time1**, which is effective from 9:00 to 12:00 and from 14:00 to 18:00 every day.

```
Hostname(config)# time-range time1
Hostname(config-time-range)# periodic daily 9:00 to 12:00
Hostname(config-time-range)# periodic daily 14:00 to 18:00
Hostname(config-time-range)# exit
```

(1) Configure an ACL to be associated with the time range.

In the time range **time1**, configure the ACL to reject any traffic from the Intranet PCs in the network segment 192.168.1.0/24 to the Internet.

```
Hostname(config)# ip access-list extended 100
Hostname(config-ext-nacl)# 10 deny ip 192.168.1.0 0.0.0.255 any time-range time1
```

Configure the ACL to allow the Intranet PCs in the network segment 192.168.1.0/24 to access the Internet in non-working hours.

```
Hostname(config-ext-nacl)# 20 permit ip any any
Hostname(config-ext-nacl)# exit
```

Apply the ACL to interface GigabitEthernet 0/1.

```
Hostname(config)# interface GigabitEthernet 0/2
Hostname(config-if-GigabitEthernet 0/1)# ip access-group 100 in
```

5. Verification

Run the **show clock** command to display the time of the device.

```
Hostname# show clock
10:14:01 beijing Sat, Dec 1, 2012
```

Run the **show time-range** command to display the time range configurations.

```
Hostname# show time-range time1

time-range entry: time1 (active)
  periodic Daily 9:00 to 12:00
  periodic Daily 14:00 to 18:00
```

Run the **show access-lists** command to display the ACL configurations. When the time of the device is in the time range **time1**, the displayed status of the ACL is active; when the time of the device is not in the effective time of ACL, the displayed status of the ACL is inactive.

```
Hostname# show access-lists
ip access-list extended 100
10 deny ip 192.168.1.0 0.0.0.255 any time-range time1 (active)
20 permit ip any any
```

Run the **show ip access-group** command to display the calling of the ACL on the interface.

```
Hostname# show ip access-group
ip access-group 100 in
Applied On interface GigabitEthernet 0/1.
```

Set the system time to working hours so that PCs in the Intranet cannot ping the Internet during working hours.

```
Hostname# show clock
14:52:26 beijing Tue, Dec 15, 2020
Hostname# ping 14.215.177.38
Sending 5, 100-byte ICMP Echoes to 14.215.177.38, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

6. Configuration Files

```
hostname Device
!
ip access-list extended 100
 10 permit ip host 10.10.10.20 any
 20 permit ip any any
!
time-range time1
 periodic Daily 9:00 to 12:00
 periodic Daily 14:00 to 18:00
!
interface GigabitEthernet 0/2
 no switchport
 ip access-group 100 in
 ip address 192.168.1.1 255.255.255.0
!
end
```

Contents

1 Configuring Supervisor Module Redundancy 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Restrictions and Guidelines 3

1.3 Configuration Task Summary 3

1.4 Configuring RDND 3

1.4.1 Overview 3

1.4.2 Configuring Manual Master/Slave Switchover 3

1.4.3 Configuring an Automatic Synchronization Period 4

1.4.4 Resetting Box-type Stacking VSU 4

1.5 Monitoring 5

1 Configuring Supervisor Module Redundancy

1.1 Introduction

1.1.1 Overview

Redundancy (RDND) is a mechanism that improves device availability by backing up the operating status of services on the supervisor module (SM) in real time.

On a network device with the control plane separated from the forwarding plane, the control plane runs on a SM and the forwarding plane runs on a line card. During the running of the device, the control plane information of the master device is backed up to the slave device in real time. When the master device is suspended as planned (for example, software is upgraded) or unexpectedly (for example, a software or hardware failure occurs), the slave device can quickly take over the work and user configurations are not lost. In this way, the network can continue to normally run. During switchover, the forwarding plane continues with forwarding; during restart of the control plane, forwarding does not stop or links do not flap.

1.1.2 Principles

1. Basic Concepts

- Global master/slave/candidate

  In a VSU system that consists of box-type devices, each box-type device is equivalent to a SM and a line card. The system also selects a device as the global master device, another as the global slave device, and other devices as global candidate devices. When the master and slave devices fail, the candidate devices take their place and run in the VSU system.

Note

- Generally, candidate devices do not participate in backup.
- A candidate device cannot directly replace the master device. When a candidate device has to become the master device, you must restart the candidate device.

- Prerequisites for the box-type stacking VSU system

  The box-type stacking VSU system works properly only when the software and hardware of all devices in the device system are compatible.

  During startup, batch synchronization must be performed between the master device and the slave device to ensure their state consistency. Before this process, the box-type stacking VSU system does not fully play its role.

- Status of the box-type stacking VSU system

  During master-slave backup, the master device has three states as follows:

  - alone, namely alone state. In this state, only one device is running in the system or master/slave switchover is not completed and no redundancy is created between the new master device and the new slave device.

- batch, namely batch backup state. Redundancy is created between the master device and the slave device and batch backup is in progress.
- realtime state, namely real-time backup state. Upon batch backup, the master and slave devices are in this state. Real-time backup is performed between the master device and the slave device. Only in this state manual switchover is allowed.

2. Selection of Master and Slave Devices

- Automatic selection of master and slave devices for the devices

  Users are allowed to add or remove devices during running of devices. Based on the current condition of the system, a device automatically selects an engine for running, without affecting normal data exchange. The master SM makes a choice in the following circumstances:

  - If only one device exists in the box-type stacking VSU environment during startup of the device, the device is selected as the master device.
  - If two devices exist in the box-type stacking VSU environment during startup of the device, by default, the device 1 is selected as the master device, the device 2 as the slave one for backup purpose and a prompt is displayed.
  - If only one device exists in the box-type stacking VSU environment during startup of the device and another is added as the slave master during the running of the device. The device added later is used as the slave one for backup purpose and outputs prompts.
  - If two devices exist in the box-type stacking VSU environment during startup of the device and either is removed during the running of the device. If the removed device is the slave one, a prompt for the removal of the slave device is displayed. If the removed device is the master one, the other device becomes the master one and displays a prompt.

- Manual selection of the master and slave devices

  Users can manually select the master and slave devices. In the box-type stacking VSU environment, users can manually perform master/slave switchover to make the global slave device become the global master device. If only two devices exist in the box-type stacking VSU environment, the original global master device becomes the new global slave one after reset. If more than two devices exist, one global candidate device is selected as the new global slave one and the original global master device becomes a global candidate one after reset.

3. Information Synchronization of Device Members

- Status synchronization

  The master device synchronizes its running status to the slave device in real time. Thus, the slave device can take over the functions of the master device at any time, without any perceivable change.

- Configuration synchronization

  During the running of the device, two system configuration files exist: **running-config**, which is dynamically generated during running and changes with the service configuration; **startup-config**, which is imported during the startup of the device. The **write** command is run to write **running-config** into **startup-config** or the **copy** command is run to copy the configuration files.

For some functions that are not directly related to uninterrupted forwarding, the synchronization of system configuration files ensures the consistency of user configurations during switchover.

In the case of the box-type stacking VSU system, the master device periodically synchronizes the **startup-config** and **running-config** files to the slave device and all candidate devices. Configurations are synchronized in the following operations:

- When a user switches from the global configuration mode to privileged EXEC mode, the **running-config** file is synchronized.
- When a user runs the **write** or **copy** command to save configurations, the **startup-config** file is synchronized.
- For configurations issued over SNMP, the **startup-config** file is not automatically synchronized and the **running-config** file must be synchronized via CLI configuration.

1.2 Restrictions and Guidelines

- For box-type devices, each device is equivalent to a SM and a line card. The VSU system of multiple box-type devices also provides the master-slave backup mechanism.

Caution

For box-type devices, box-type stacked VSUs are used to express the redundancy mechanism.

1.3 Configuration Task Summary

RDND configuration includes the following tasks:

All of the following configuration tasks are optional. Select the task as required.

- (Optional) Configuring Manual Master/Slave Switchover
- (Optional) Configuring an Automatic Synchronization Period
- (Optional) Resetting Box-type Stacking VSU

1.4 Configuring RDND

1.4.1 Overview

- The device automatically selects the master and slave devices based on the current system, or users do so manually.
- In the box-type stacking VSU environment, the master device synchronizes status information and configuration files to the slave device in real time.

1.4.2 Configuring Manual Master/Slave Switchover

1. Overview

If more than two devices exist in the system, you can manually perform master/slave switchover to change the slave device into the master device and select a new slave device from candidate devices (the original master device becomes a candidate device after reset).

2. Restrictions and Guidelines

- To ensure smooth data forwarding during switchover, perform batch synchronization performed between the master device and the slave device so that the two modules are in the same state. That is, manual switchover is allowed only when the redundancy of the box-type stacking VSU is in the real-time backup state. In addition, manual master/slave switchover is temporarily disabled by service modules during synchronization to ensure that configuration files are completely synchronized. Therefore, manual master/slave switchover is enabled on the master device and the slave master exists.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Perform a master/slave switchover.

redundancy forceswitch

1.4.3 Configuring an Automatic Synchronization Period

1. Overview

By configuring an automatic synchronization cycle, you can adjust the interval for the master device to synchronize the configuration files (**startup-config** and **running-config**) to change the automatic synchronization period.

2. Restrictions and Guidelines

It is recommended that a short synchronization period be configured so that the master device can frequently synchronize configurations to other member devices when configurations are modified. In this way, the configurations are not lost when services and data are forcibly switched to the slave device due to the failure of the master device.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the redundancy configuration mode.

redundancy

(4) Configure a period for automatically synchronizing configuration files.

auto-sync time-period *synchronization-interval-time*

The default period for automatically synchronizing configuration files is 1 hour.

1.4.4 Resetting Box-type Stacking VSU

1. Overview

- Resetting only the slave device does not affect data forwarding. During the resetting of the slave device, forwarding is not interrupted or user session information is not lost.

- In standalone mode, running the **redundancy reload shelf** command makes the device reset; in VSU mode, this command is used to reset the device with a specified ID. If two or more devices exist in the system and the device where the global master SM resides is reset, the system performs master/slave switchover.

2. Restrictions and Guidelines

In the box-type stacking VSU mode, if the SMs of the system are not in the real-time backup state, resetting the device where the global master SM resides will cause the whole VSU system to reset.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Reset the box-type stacking VSU.

redundancy reload { **peer** | **shelf** [*switch-id*] }

1.5 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 RDND Monitoring

Command	Purpose
show redundancy states	Displays the current redundancy status of the device.

Contents

1 Configuring Process Restarting 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Restrictions and Guidelines 1

1.3 Configuration Task Summary 1

1.4 Configuring RAS-CMDK 2

1.4.1 Overview 2

1.4.2 Restarting a Process of the Member Device in a Specified Slot on a Specified Device 2

1.4.3 Starting a Process of the Member Device in a Specified Slot on a Specified Device 2

1.4.4 Stopping a Process of the Member Device in a Specified Slot on a Specified Device 2

1.4.5 Displaying Processes that can Be Restarted on the Member Device in a Specified Slot on a Specified Device 3

1.5 Monitoring 3

1 Configuring Process Restarting

1.1 Introduction

1.1.1 Overview

The command line interface (CLI) reboot process module (CMDK) provides a means of restarting a back-end process of a device on the CLI for users. Therefore, when the function of a service fails on a device, the user can restart a specified process of the member device in a specified slot on a specified device in a cluster rather than restart the device, to improve device availability.

The CMDK has the following features:

- Improve the device availability. When a process in a device becomes abnormal, users can manually restart a specified process.
- Support process restart in the virtual switching unit (VSU) environment. The CMDK can restart a specified process of the member device in a specified slot on a specified device. Therefore, users can restart a process on the master device or master supervisor module.

1.1.2 Principles

First, a process determines whether the current device is in the standalone or VSU environment. Then, the process sends a process kill message to a target node. After receiving the message, the target node restarts the whole process by running the command in the startup script.

1.2 Restrictions and Guidelines

Configuration commands are run on only the master device or master supervisor module. Other member devices do not have the permission to run the commands.

1.3 Configuration Task Summary

The RAS-CMDK configuration includes the following tasks: The following configuration tasks are optional. Configure the task as required.

- Restarting a Process of the Member Device in a Specified Slot on a Specified Device
- Starting a Process of the Member Device in a Specified Slot on a Specified Device
- Stopping a Process of the Member Device in a Specified Slot on a Specified Device
- Displaying Processes that can Be Restarted on the Member Device in a Specified Slot on a Specified Device

1.4 Configuring RAS-CMDK

1.4.1 Overview

The CLI CMDK provides a means of restarting a back-end process of a device on the CLI for users. Therefore, when the function of a service fails on a device, the user can restart a specified process of the member device in a specified slot on a specified device in a cluster rather than restart the device, to improve device availability.

1.4.2 Restarting a Process of the Member Device in a Specified Slot on a Specified Device

1. Overview

This section describes how to restart a specified process on a specified device.

2. Restrictions and Guidelines

Only valid processes excluded from the whitelist can be restarted.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Restart a process of the member device in a specified slot on a specified device.

cmdk device *device-id* **slot** *slot-id* **module** *module-name* **restart**

1.4.3 Starting a Process of the Member Device in a Specified Slot on a Specified Device

1. Overview

This section describes how to start a specified process on a specified device.

2. Restrictions and Guidelines

Only valid processes can be started.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Start a process of the member device in a specified slot on a specified device.

cmdk device *device-id* **slot** *slot-id* **module** *module-name* **start**

1.4.4 Stopping a Process of the Member Device in a Specified Slot on a Specified Device

1. Overview

This section describes how to stop a specified process on a specified device.

2. Restrictions and Guidelines

Only valid processes excluded from the whitelist can be stopped.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Stop a process of the member device in a specified slot on a specified device.

cmdk device *device-id* **slot** *slot-id* **module** *module-name* **stop**

1.4.5 Displaying Processes that can Be Restarted on the Member Device in a Specified Slot on a Specified Device

1. Overview

This section describes how to display processes that can be restarted on the member device in a specified slot on a device.

2. Restrictions and Guidelines

The processes that can be restarted on the member device in a specified slot are displayed only on the master device.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Display the processes that can be restarted on the member device in a specified slot on a specified device.

cmdk device *device-id* **slot** *slot-id* **detail**

1.5 Monitoring

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 RAS-CMDK Monitoring

Command	Purpose
debug cmdk on	Enables the CMDK debugging mode.
debug cmdk off	Disables the CMDK debugging mode.

Contents

1 Configuring Module Hot Swapping 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Working Principle 1

1.2 Users can insert or remove a module (in hot swapping mode) when a device is operating. The operation of other modules is not affected. After a module is inserted into a slot, the management software of the device tries to install the driver of the module automatically. The configuration of a removed module is retained for future configuration. If a removed module is inserted again, the module is automatically started and its configuration becomes effective. Clearing and Modifying Module/Device Configurations 1

1.2.1 Overview 1

1.2.2 Procedure 2

1.3 Monitoring 2

1 Configuring Module Hot Swapping

1.1 Introduction

1.1.1 Overview

Module hot swapping is a maintenance function. With this function, users can insert or remove a module when a device is operating.

The module hot swapping function supports automatic installation, unloading, reset, and information query of various hot-swappable modules (including line cards, and VSU members).

1.1.2 Working Principle

1. Automatic Installation of an Inserted Module

Users can insert or remove a module (in hot swapping mode) when a device is operating. The operation of other modules is not affected. After a module is inserted into a slot, the management software of the device tries to install the driver of the module automatically. The configuration of a removed module is retained for future configuration. If a removed module is inserted again, the module is automatically started and its configuration becomes effective.

1.2 Clearing and Modifying Module/Device Configurations

1.2.1 Overview

In different circumstances, different configurations need to be cleared. The specific application scenarios are described as follows:

- Clearing the configurations of a module; A user inserts a board card into a slot on a device. Later, the user removes the board card and deletes the configurations of the board card and its port because the board card is no longer used.
- Clearing the configuration of a VSU member device: A user uses a member device in a VSU. Later, the user removes the device from the VSU and deletes the configurations of the member device in the VSU.
- Deleting the MAC address retained in the configuration file: A user hopes to change the MAC address of the system and uses the new MAC address elected by the system. Generally, the MAC address used by the system is stored in the Supervisor Engine or flash memory of the chassis. In VSU mode, however, the system automatically stores the used MAC address in the configuration file to avoid interruption caused by the change of the MAC address. If a valid MAC address exists in the configuration file after restart of the device, the MAC address is used in preference.
- Modifying the MAC address retained in the configuration file; The function is used when the system MAC address of a device needs to be modified. In gateway mode (the **auth-mode gateway** command is configured in the system), the gateway MAC address is bound on some peripheral devices. If the gateway is replaced, users can run the **sysmac** command to set the gateway MAC address to the MAC address of the new gateway so that configurations do not need to be modified for downstream devices with the gateway MAC address bound. The **sysmac** command is available only when the system is configured to work in

gateway mode.

1.2.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Clear the configuration of a VSU member device.

remove configuration device *device-id*

(4) (Optional) Modify the MAC address retained in the configuration file.

sysmac *mac-address*

No MAC address is specified for the system by default.

.

1.3 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show version module detail [*slot-num*] **show version module detail** [*device-id / slot-num*] (in VSU mode)	Displays the details of a module.
show version slots [*slot-num*] **show version slots** [*device-id / slot-num*] (in VSU mode)	Displays the online status of a module.
show manuinfo	Displays the asset information of all independent components in the current system.
show sysmac	Displays the current MAC address of the system.
show alarm	Displays system-level alarms.
show device-level	Displays the application level of the current device.

Contents

1 Configuring Python.....1

1.1 Introduction.....1

1.1.1 Overview.....1

1.1.2 Principles.....1

1.2 Restrictions and Guidelines.....1

1.3 Configuring Basic Features.....1

1.3.1 Overview.....1

1.3.2 Procedure.....1

1 Configuring Python

1.1 Introduction

1.1.1 Overview

Python is an object-oriented interpretive computer programming language and is pure free software. Its source code and interpreter Cpython comply with GNU general public license (GPL) protocol. The Python shell component can debug and run Python scripts through CLI commands.

1.1.2 Principles

1. Python Script Debugging

Python script debugging refers to debugging or running a script to be run on a device. A Python script is debugged with two methods:

- One is to copy the Python script to a device and debug the script on the Python console.
- The other is to copy the Python script to a device and run the script. Check whether the expected effect is achieved. If not, modify and debug the script.

Regardless of methods, the user runs an open source Python command and the debugging method is consistent with that of the open source Python. The Python shell component redirects the input and output of the open source Python process to the current terminal.

2. Permission Control

Permission control indicates that Python CLI commands are not allowed to operate directories or files other than **flash:** and **tmp:** and risky operations such as popen and system are not allowed in a script.

Permissions are controlled at the entry of Python. So long as a Python script is run on a device, permissions are controlled to control the risk caused by running of the Python script.

1.2 Restrictions and Guidelines

Permission control: Python commands and scripts can be run on only files in the **flash:** and **tmp:** directories.

1.3 Configuring Basic Features

1.3.1 Overview

This section describes how to run a Python script.

1.3.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Debug a Python script.

python *file-name* [*args*]

Contents

1 Configuring License Management 1
1.1 Introduction 1
1.1.1 License Management Overview 1
1.1.2 Principles 1
1.2 Configuration Task Summary 4
1.3 Configuring License Management 4
1.3.1 Overview 4
1.3.2 Installing License File 4
1.3.3 Backing Up License File 5
1.3.4 Configuring Grace Period Warning 6
1.3.5 Updating License File 6
1.3.6 Uninstalling License 7
1.3.7 Unbinding License 7
1.4 Monitoring 8

1 Configuring License Management

1.1 Introduction

1.1.1 License Management Overview

A user needs to install a correct license file to use some extension functions of a device. The extension functions provided by Ruijie General Operating System (RGOS) include the virtual switch device (VSD), Transparent Interconnection of Lots of Links (TRILL) and Fibre Channel over Ethernet (FCoE), and user concurrency supported by virtual private network over Secure Sockets Layer (SSLVPN). A user can use the general and extension functions of the RGOS only after obtaining a license.

Note

Generally, all features of the RGOS are pre-installed in the factory. For feature licenses and license types, see their configuration guides. RGOS features or basic functions that are not expressly specified can be used directly without licenses.

1.1.2 Principles

1. Basic Concepts

- Software to be licensed

  A software function used by only a licensed user.

- Feature license

  As a license for a special feature, it is obtained through a license file, hardware entity, or legal contract. This license specifies the maximum number of supported users, the maximum number of supported instances, and valid period.

- Product authorization key (PAK)

  It is a manner of granting a license to a user by providing a license code.

- Purchase voucher

  A voucher of purchasing a license. The voucher contains the PAK and license download address. The legitimate owner of the purchase voucher logs in to the license download address, and uses the PAK to sign up. The license file is downloaded from the displayed link or is directly sent to the registered email.

- Host ID

  A unique serial number for identifying each device.

Caution

A license matches the host ID of any device added to a VSU. When the device is removed from the VSU, the feature enabled by the license becomes invalid.

- License file

A file that controls the features of a licensed software. A license file is generated by using a special tool based on contract information, and each license file contains a digital signature to prevent tampering. The license file serves a product. That is, one license file is used on only one device and matches the device's host ID. License is not transferred. Licensed functions are available when the license file is installed.

- Temporary license

  A temporary license becomes invalid after the valid period expires.

- Evaluation license

  An evaluation license is temporary, and has been installed on the device before delivery. It is used to provide users with features for trial use. This type of license is independent of the host ID.

- Permanent license

  This license has no time limit and is permanently effective upon purchase by the user.

- License stacking

  Different licenses can be used on one device. For example, if a device provides both the FCoE and TRILL functions, users can purchase the licenses of the two functions and use them on the same device.

- Single-Instance license

  Only one license can be installed for one feature at a time.

Caution

Licenses for the features like user concurrency supported by VSD, TRILL, FCoE, and SSLVPN are all single-instance licenses.

- Multi-instance license

  Multiple license files can be installed for the same feature on a device.

Caution

Only the license for the feature "user connections supported by the AP" is a multi-instance license.

- Grace period warning

  A grace period warning is generated in forms of log and trap messages 180 days before a license expires. Setting a grace period warning prevents licensed software from being affected when an aging license suddenly stops working upon expiration.

2. License Acquisition and Use

- Use of License

  A license must be obtained from Ruijie's official website or marketing channel. It is device-specific. You log in to the website specified in the purchase voucher and provide the PAK and host ID to obtain the license file, which is directly downloaded or given through an email. After acquisition, you need to install the license file. Afterwards, you can use the features of the license.

  RGOS licenses include permanent license and temporary license. When a user first enables a temporary license to use a feature, the valid period of the license starts, and after the period ends, the feature will be

disabled. To continue using this feature, this user can purchase another license (permanent or temporary) from Ruijie's official website or marketing channel.

Caution

In the VSU environment, multiple devices form one virtual device. In this scenario, if one device obtains the license for a feature, the whole VSU is licensed to use this feature. But when the devices in the VSU are separated, the license is checked by device.

The VSD function provided by the RGOS helps divide one RGOS device into multiple virtual devices. For external users, each virtual device works like an independent device. That is, when the license for a feature is obtained, the license for this feature is effective to all VSD domains. In addition, licenses are installed and managed in the default VSD only.

- License check

  After a device starts to run, the license for each feature needs to be checked. If the corresponding license is properly installed, this feature is ready for application. Otherwise, this feature becomes invalid and cannot be used.

  Note

  Checking the licenses for various features occurs at different times. The licenses for some features are checked during startup, and the licenses for other features are checked in real time.

- Loss of License File

  License files are stored in the **/data** directory of a device and is not lost after software upgrade.

  If the memory or file system is damaged during product use but the license file has been backed up, you can install the backup license file again after system recovery. If the license file is not backed up, you can visit Ruijie's website to obtain the license file again. This process is the same as the previous acquisition process (you do not need to purchase the license again).

  Licensing is device-based. After a license is provided for a specified device, the license file is verified only on this device. Upon maintenance or replacement of a device, the host ID may change and the obtained license file may not be identified. In this case, contact Ruijie after-sales personnel.

3. Backup, Update, and Uninstallation of a License File

- License File Backup

  When a fault such as damage of file system storage media occurs on a device, the license file on this device may be lost after you troubleshoot this fault. Therefore, you need to back up the license file in advance to reinstall it after you troubleshoot the fault.

- License File Update

  If the existing license of the system fails to meet the feature requirements, you can visit Ruijie's website to purchase a desired license and then update the license file locally.

- License File Uninstallation

If you do not need a feature, you can uninstall the license for this feature to improve the utilization of resources like the memory. To reuse this feature, reinstall the license. It is recommended that license files be kept properly.

1.2 Configuration Task Summary

Configuration of license management includes the following tasks:

(1) Installing License File

(2) Backing Up License File

(3) (Optional) Grace Period Warning

(4) (Optional) Updating License File

(5) (Optional) Uninstalling License

(6) (Optional) Unbinding License

1.3 Configuring License Management

1.3.1 Overview

This section describes how to enable or disable a feature by installing or uninstalling a license file.

1.3.2 Installing License File

1. Overview

This section describes how to install a license file to enable a licensed feature.

2. Restrictions and Guidelines

- Ruijie provides a paper purchase voucher that contains a PAK when you purchase a license.
- Log in to Ruijie's website and obtain a license file as prompted.
- If you use a feature without being licensed, the CLI window displays a prompt, indicating that the feature is not licensed and is unavailable, and provides a website to download a license file.
- After downloading a license file from the specified website, upload this license file to the device (or store it in a USB flash drive) for installation. You can install the license file offline. Copy the license file to the file system of the device. Use conventional file system operation commands. For example, download the license file through Trivial File Transfer Protocol (TFTP) or copy the license file to a USB flash drive.
- After a license file is installed on a device, this license file is automatically backed up in the **/data** directory of the system (the license file is suffixed with **.lic**). The backup license file is deleted when the installed license is uninstalled.
- In a VSU environment, run the **license install** command on a master supervisor module to install the license file on all devices, or run this command on a non-CM supervisor module to install the license file only on the device from which you enter commands.
- In a VSU environment, run the **license auto-install** command to automatically match compliant devices to install the license file. In a non-VSU environment, run the following commands to do the same:
- In a VSU environment, when the license for a feature is obtained by one device by running the **license**

install command, the whole VSU system is licensed to use this feature. But when the devices in the VSU are separated, the licensed device can still use the license.

- In a VSU environment, run the **license install** command on a CM supervisor module to install a license on all boards, or run the **license auto-install** command on a CM supervisor module to install a license on a matched board only. Run the **license install** command on a non-CM supervisor module to install a license on the local device, or run the **license auto-install** command on a non-CM supervisor module to automatically match and install a license on all devices.
- The **license auto-install** command enables the auto-matching function only in a VSU environment, and has the same function as the **license install** command in other environments.
- In a VSD environment, licenses are managed in global configuration mode. When the license for a certain feature is obtained, the license for this feature is effective to all VSD domains. In addition, licenses are installed and managed in the default VSD only.
- Different devices do not share the same license file.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Obtain **host-id** of the device.

show license hostid

The name of a license file cannot be modified.

This command can be executed without permission.

(3) (Optional) Install the license file. Please select either configuration.

- Install a license manually.

license install { **flash**: | **usb**0: } *filename*

- Install a license automatically.

license auto-install { **flash**: | **usb**0: } *filename*

1.3.3 Backing Up License File

1. Overview

This section describes how to back up the license files of one or all features in the system.

2. Restrictions and Guidelines

- Evaluation license files cannot be backed up.
- Sufficient storage space is required to store backup license files. Generally, one license file is 4 KB to 10 KB.
- Backup license files are normal files.
- When all license files in the system are backed up, a .tar file is generated.
- You can run the **dir** command to save the license files to other storage devices, for example, a USB flash drive.
- After backing up license files, you can run the **dir** command to confirm the generated license files, and compare them with the license file names displayed in the **installed license** fields of permanently licensed

features in the command output of the **show license all-license** or **show license file** command, to check whether licenses are correctly backed up.

- The **installed license** field displayed in the **show license all-license** command and **show license file** command is available only for multi-instance licenses. The name of a file internally backed up in the multi-instance license system is determined by the ID of the multi-instance license. One single-instance license file exists at most in the system at a time. Therefore, the internally backed up single-instance license file is named after the feature.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Back up the license files in the system.

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

1.3.4 Configuring Grace Period Warning

1. Overview

This section describes how to evaluate the expiration date of a license and how to provide early warnings in form of log messages to remind users of taking actions in advance.

2. Restrictions and Guidelines

- Each licensed feature is separately configured.
- The grace period warning is affected by the device time.
- A permanent license file needs no grace period warning.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Set the grace period warning for a licensed feature.

license grace-period *filename days*

The grace period before the expiration of a license is 180 days by default.

1.3.5 Updating License File

1. Overview

This section describes how to update the license file for a feature of the system. Generally, this function is performed to update an evaluation license file into a temporary license file.

2. Restrictions and Guidelines

- A formal permanent license file does not need to be updated.
- A later license version cannot be updated into an earlier one.
- A license file contains a generation time field. The value of this field is the time when the license file is generated on the website. When the value is closer to the current time, the license file has a later version.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Update the license file.

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

1.3.6 Uninstalling License

1. Overview

This section describes how to uninstall one or all feature licenses in the system when the features are not needed.

Note

This function becomes invalid when the corresponding license is uninstalled.

2. Restrictions and Guidelines

- If the licensed feature is running, the uninstallation does not take effect immediately, but takes effect after the feature is enabled or restarted next time.
- You are advised to back up a license file before uninstallation to reinstall an uninstalled license when needed.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Uninstall a license in the system.

license auto-uninstall *devid license* [*filename*]

This command can be executed without permission.

1.3.7 Unbinding License

1. Overview

If you want to unbind a license from a device on the license website, unbind the license on the device first.

2. Restrictions and Guidelines

- Upon unbinding a license, you obtain a verification code, which is used to unbind the license on the license website.
- After the license is unbound, the corresponding license file cannot be reinstalled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Unbind a license in the system.

license unbind *pak*

This command can be executed without permission.

1.4 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show license all-license	Displays the list of all installed license files on the device.
show license file *file-license*	Displays the information about a specified license file on the device.
show license dev-license	Displays license configurations of all devices.
show license usage	Displays licenses in use.
show license hostid	Displays the device SN used for licensing.
show license dev-hostid	Displays the device SN of each device
show license unbind-code	Displays the verification code of a license unbound from the device.
show license dev-unbind-code	Displays the verification code of a license unbound from each device in the environment.

Virtualization Configuration

1. VSU Configuration

Contents

1 Configuring VSU....1
1.1 Introduction....1
1.1.1 Basic Concepts....1
1.1.2 VSU Application....4
1.1.3 VSU Topology....7
1.1.4 DAD....9
1.1.5 Traffic Forwarding....11
1.1.6 System Management....12
1.1.7 System Upgrade....13
1.1.8 Quick Blinking Location....13
1.2 Restrictions and Guidelines....13
1.3 Configuration Task Summary....14
1.4 Setting Up a VSU....14
1.4.1 Overview....14
1.4.2 Restrictions and Guidelines....14
1.4.3 Prerequisites....14
1.4.4 Procedure....14
1.5 Configuring BFD-based DAD....15
1.5.1 Overview....15
1.5.2 Restrictions and Guidelines....15
1.5.3 Prerequisites....16
1.5.4 Procedure....16

1.6 Configuring AP-based DAD 17
1.6.1 Overview 17
1.6.2 Restrictions and Guidelines 17
1.6.3 Prerequisites 17
1.6.4 Procedure 17
1.7 Configuring the VSL 18
1.7.1 Overview 18
1.7.2 Restrictions and Guidelines 18
1.7.3 Prerequisites 18
1.7.4 Procedure 18
1.8 Configuring VSU Attributes 19
1.8.1 Overview 19
1.8.2 Configuration Tasks 19
1.8.3 Configuring Basic VSU Attributes 19
1.8.4 Configuring Traffic Balancing 20
1.8.5 Switching to Standalone Mode 21
1.8.6 Configuring Recovery Method for Recovery Mode 21
1.9 Configuring Quick Blinking Location 22
1.9.1 Overview 22
1.9.2 Restrictions and Guidelines 22
1.9.3 Procedure 22
1.10 Monitoring 22
1.11 Configuration Examples 23
1.11.1 Setting Up a VSU 23

1.11.2 Configuring BFD-based DAD 25

1.11.3 Configuring AP-based DAD 28

1.12 Common Misconfigurations 32

1 Configuring VSU

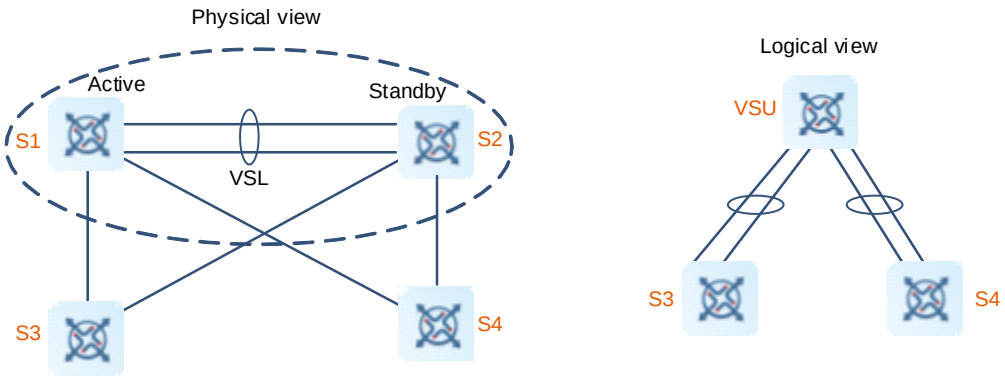
1.1 Introduction

Virtual Switching Unit (VSU) is an N:1 network device technology independently developed by Ruijie. It simplifies the device operation & maintenance (O&M) and network topology by virtualizing multiple network devices into a single logical device for management and use. In addition, the VSU technology connects peripherals to different member devices in the VSU through aggregated links to achieve cross-device link redundancy and improve reliability and scalability of networks.

1.1.1 Basic Concepts

As shown in Figure 1-1, the left part shows the physical view of devices that form a VSU, which is equivalent to one logical device.

Figure 1-1 Schematic Diagram of VSU



1. VSU

The VSU is a single logic entity composed of multiple redundant devices in a conventional network structure. The devices on the access layer, the distribution layer, and the core layer can form the VSU.

2. Domain ID

A domain ID is the unique identifier of a VSU and distinguishes different VSUs. Only two devices that share the same domain ID can compose a VSU.

3. Device ID

Each device in a VSU is called a member device, and each member device has a unique device ID, i.e. switch ID. This device ID is used to manage the member device and configure interfaces on the member device. When adding the device to a VSU, you need to configure an ID for a device and ensure that the ID is unique in the same VSU. If device IDs of member devices conflict in a VSU, only one device is retained according to rules.

4. Device priority

Priority is an attribute of a member device, and is used to elect a role. A higher priority indicates a higher probability of being elected as the active device. To elect a device as the active device, increase its priority. Member devices have two types of priorities.

- Configuration priority: priority stored in the configuration file, which is changed at any time, and takes effect after the configurations are saved and the VSU is restarted.
- Running priority: configuration priority stored in the configuration file at the startup, which does not change during VSU running.

5. Device role

Member devices are assigned with three roles based on their functions:

- Active device: Manages and controls the entire VSU. Only one active device exists in a VSU domain.
- Standby device: Serves as a backup of the active device and participates in data forwarding only. All received data packets are forwarded to the global active device for processing. When the active device is faulty, the standby device automatically switches to the active mode and takes over functions of the original active device.
- Candidate device: Serves as a backup of the standby device and participates in data forwarding only. When the standby device is faulty, the system automatically elects a new standby device from candidate devices to take over functions of the original standby device. When the active device is faulty and the standby device switches to the active mode, the system automatically elects a new standby device from candidate devices.

6. Role election

A VSU is composed of at least the active device and standby device. When it is composed of more than two devices, the other devices are candidate devices. Role election applies to the following scenarios:

- VSU setup
- Device fault or exit from a VSU
- VSU splitting
- VSU combination

Roles are elected based on the following rules:

- The active device is elected by priority. The device priorities are ranked as follows:

  Current active device (no active device exists upon startup) > Device with a higher priority > Device with a smaller ID > Device with a smaller MAC address
- A device directly connected to the active device is preferentially elected as the standby device to avoid dual active devices. The device priorities are ranked as follows:
  Device directly connected to the active device > Device with a higher priority > Device with a smaller MAC address

Note

- When a device joins an existing VSU in hot mode, the system does not switch between the active and standby roles, even if the device has a higher priority than the active and standby devices in the running VSU.

- The startup sequence of member devices may affect the election of the active device. A member device may not join the VSU in time due to slow startup (the current VSU directly converges if it does not discover a neighbor within 5 minutes). In this case, the member device joins the VSU in hot mode, and the system does not switch active/standby role even if the member device has a higher priority than the active device in the current VSU.
- A candidate device is elected as a standby device only.

7. Virtual switching link

The VSU is a network entity of multiple devices that need to share control information and data flows. Virtual Switching Link (VSL) is a special link used to transmit control information and data flows between the devices in the VSU. Figure 1-1 shows the locations of VSLs in the VSU.

A VSL usually exists in the form of aggregation port group, and a data flow transmitted by the VSL is load-balanced among the aggregation port members based on a traffic balancing algorithm.

- VSL traffic

Control flows transmitted by the VSL between devices are classified into the following two types:

  - Protocol packets received by a member device, which are forwarded through the VSL to the global active device for processing.
  - Protocol packets processed by the global active device, which are forwarded through the VSL to the interfaces of other member devices and then sent to the peer devices by these interfaces.

The data flows transmitted through the VSL between devices include:

  - Flooding data flows in a VLAN
  - Data flows that need to be forwarded across devices and transmitted through the VSL

A VSL also transmits internal management packets of the VSU, for example, protocol information of hot backup devices, and packets that carry configurations to be delivered from the active device to other member devices.

- CRC error detection of VSL port

When a VSL port has many consecutive Cyclic Redundancy Check (CRC) errors, disable this port and switch to another VSL port. CRC errors are handled according to the following rules:

  - The VSL port is checked for CRC errors every 5 seconds by default. If the number of CRC errors incremented between one check and the latest check is greater than the threshold of CRC errors (the *error-number* parameter), one CRC error occurrence is counted.
  - When the number of consecutive CRC errors exceeds the configured number (the *time-number* parameter), the port is abnormal.
  - If there are multiple VSLs and CRC errors occur in only one link, VSL is switched. If there are multiple VSL links and CRC errors occur in the last normal VSL, the link is not switched to prevent topology splitting.
  - The values of *error-number* and *time-number* vary with the scenario. The default values of *error-number* and *time-number* are **3** and **10** respectively. In scenarios with high tolerance for CRC errors, reduce the two recommended parameter values; otherwise, increase them.

- VSL recovery

By default, a device automatically restarts and joins the VSU again after a VSL fault is rectified. If the automatic restart function is disabled, you must enable this function or directly restart the device after the VSL fault is rectified to rebuild the VSU.

1.1.2 VSU Application

Compared with conventional networks, VSU has the following advantages:

- Low cost: lightweight and dynamic network capacity expansion for protecting the equipment investment in the existing network, and reducing the construction cost.
- Simple O&M: reduced management workload, simplified networking, and lowered O&M difficulty.
- High reliability: device and link redundancy mechanisms for improved network reliability.

1. Flexible expansion

Capacity expansion applies to the following scenarios:

- Port expansion: The port density of the existing access switch cannot meet the requirement of increasing access users, as shown in Figure 1-2.
- Forwarding capacity expansion: The forwarding capacity of the existing core switch cannot meet the requirement of increasing services, as shown in Figure 1-3.
- Bandwidth expansion: The uplink bandwidth cannot meet the demand in peak hours, as shown in Figure 1-4.

The above problems are solved by adding a switch to form a VSU with the original switch. Physically, the two switches seem to be one, and the original switch backs up and sends the current configurations in batches to the new switch. Therefore, this change has little impact on network planning and configuration. The VSU features the following:

- Higher port density: The VSU forwards data as a whole, and the new switch is equivalent to a port expansion card of the original switch to increase port density.
- Higher forwarding capacity: If one switch has a forwarding capacity of 14,400 Mpps, the entire VSU has a forwarding capacity of 28800 Mpps after one switch is added.
- Larger bandwidth: If a 1000 M switch needs to perform 10 G uplink connection but provides only two 10G ports, up to 20 Gbps uplink bandwidth is supported. By adding one switch of the same type to set up a VSU, you can configure four 10 G ports into one aggregation group to increase the uplink bandwidth to 40 Gbps.

Figure 1-2 Port Expansion over VSU

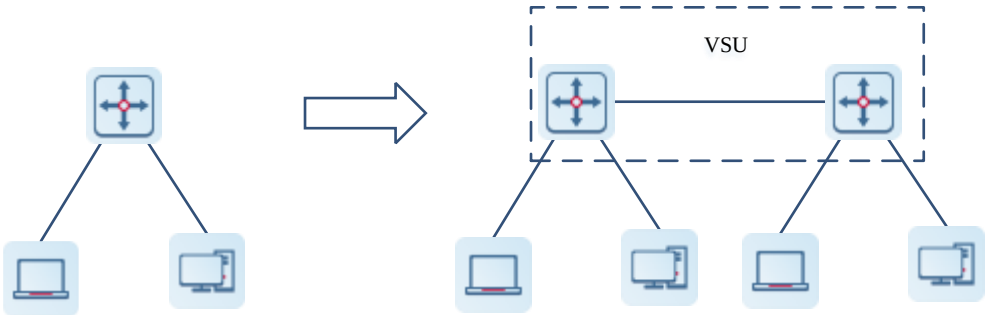


Figure 1-3 Forwarding Capacity Expansion over VSU

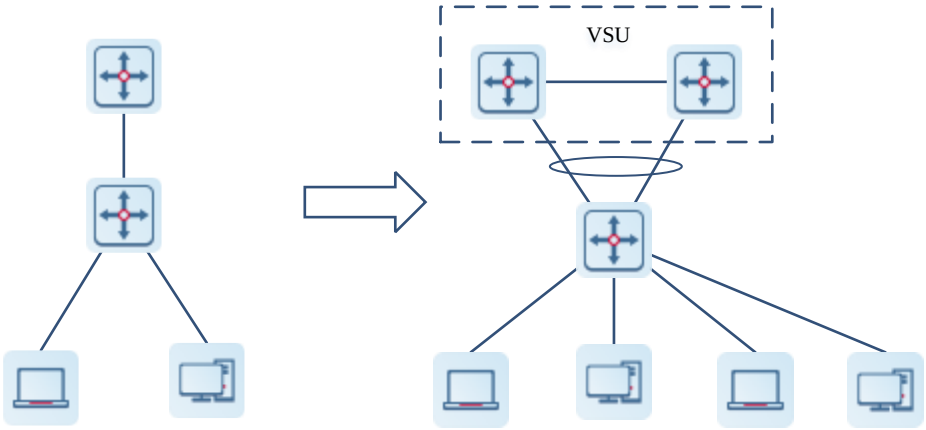
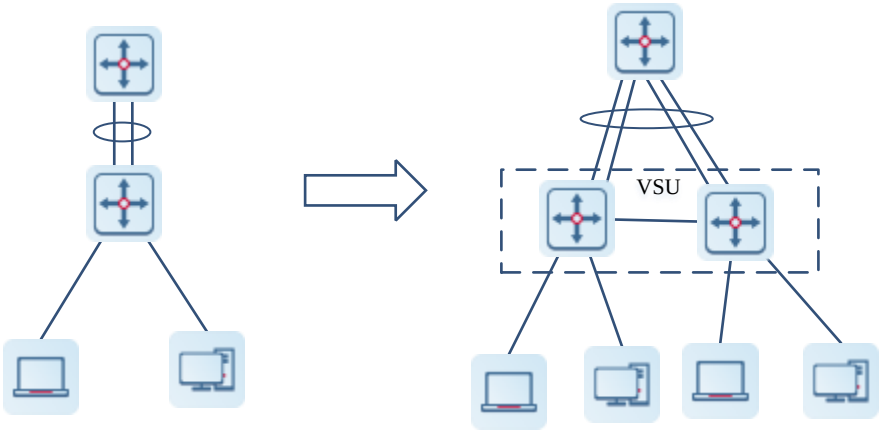


Figure 1-4 Bandwidth Expansion over VSU

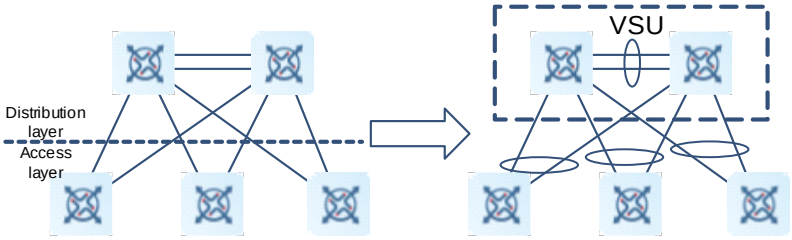


2. Simplified management

Simplified management is reflected in the following aspects:

- Device: After multiple devices form a VSU, an administrator can manage them together, without connecting to them for separate configuration and management. If a VSU is deployed between two floors/buildings, only one distribution device is needed between the floors/buildings, and this reduces the management and O&M costs.
- Networking: Figure 1-5 shows a common networking mode. Typically, each access switch is connected to two distribution switches to improve network reliability. The entire network topology is complex and has a loop. You also have to enable protocols such as Multiple Spanning Tree Protocol (MSTP) and Virtual Router Redundancy Protocol (VRRP) to eliminate the loop and support gateway backup. To meet the traffic balancing requirement, multi-loop network technologies such as Ethernet ring protection switching (ERPS) also need to be enabled. As a result, the configuration is complex, and the maintenance is difficult and prone to errors. After a VSU is formed, MSTP, VRRP, and ERPS are not required. Only the common link aggregation function can balance traffic , eliminate loops, and provide cross-device link redundancy, thus simplifying the topology and making deployment easier.

Figure 1-5 Simplified Networking over VSU



3. Hot backup

As shown in Figure 1-6, two switches form a VSU to provide the following redundancy to adapt to high reliability scenarios:

- Device redundancy: redundancy between member devices in the VSU. Failure of the standby device does not affect the entire system, but failure of the active device makes the system switch to the standby device. This switching is similar to the dual-engine switching of a standalone device. Such switching is completed within milliseconds, without interrupting services (TCP flows rely on the retransmission mechanism to ensure service continuity).
- Link redundancy: A switch connects to surrounding devices through aggregated links, which provides cross-device link redundancy, implements load balancing, and fully utilizes all bandwidth. If one member link fails, the system switches to another member link within milliseconds.

Figure 1-6 Hot Backup over VSU

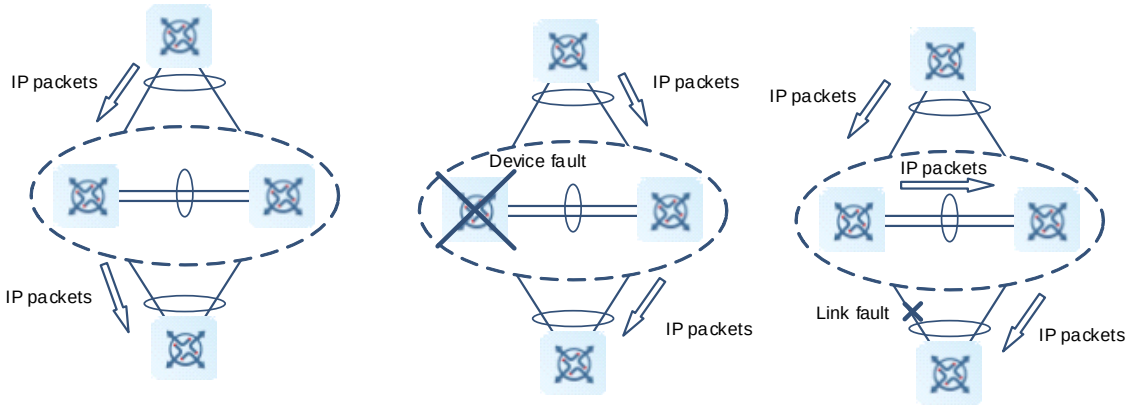
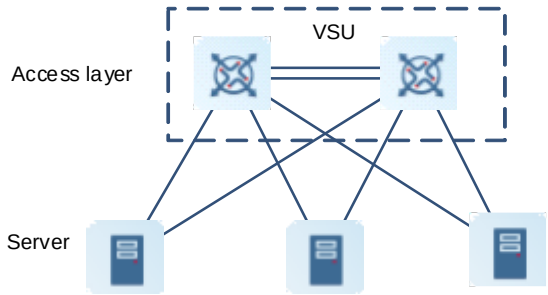


Figure 1-7 shows the typical application scenarios. Access servers with high availability requirements are connected with devices on the access layer by binding multiple network interface cards of a single server into an aggregation port. As the aggregation port allows access to only one access device, the risk of failure of the single device increases. In this case, setting up a VSU enables the server to connect to member devices in the VSU over the aggregation port. This deployment prevents network interruption caused by the single point of failure of the access device or the failure of a single link, and improves network reliability of services carried by the server.

Figure 1-7 Server Access Link Redundancy



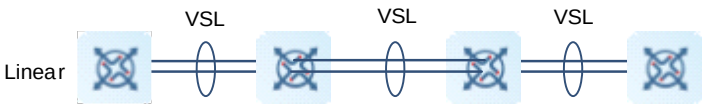
1.1.3 VSU Topology

A VSU supports linear topology and ring topology.

1. Linear topology

As shown in Figure 1-8, devices are connected through a VSL to form a line, and this topology is therefore called linear topology. The linear topology is simple. It uses a few ports and cables. Two devices are connected with a communication link only. Therefore, the VSL is less reliable.

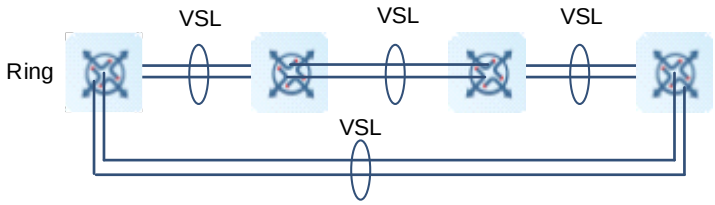
Figure 1-8 Linear Topology



2. Ring topology

In the ring topology shown in Figure 1-9, the two communication links backed up by each other form link redundancy, which improves the reliability of the VSU.

Figure 1-9 Ring Topology



Note

- The ring topology is recommended for the VSU, to ensure that the failure of any single device or any single VSL link does not affect the normal operation of the entire VSU.
- Besides, you are advised to configure multiple VSLs to improve reliability. You are advised to configure at least two VSLs.

3. Topology convergence

During setup of the VSU, the management scope is determined through topology convergence. The process is as follows:

(1) The member devices discover their neighbors through a topology discovery protocol to determine the list of devices included in the VSU.

(2) The global active device is elected to manage the entire VSU.

(3) The global standby device is elected as the backup for the active device.

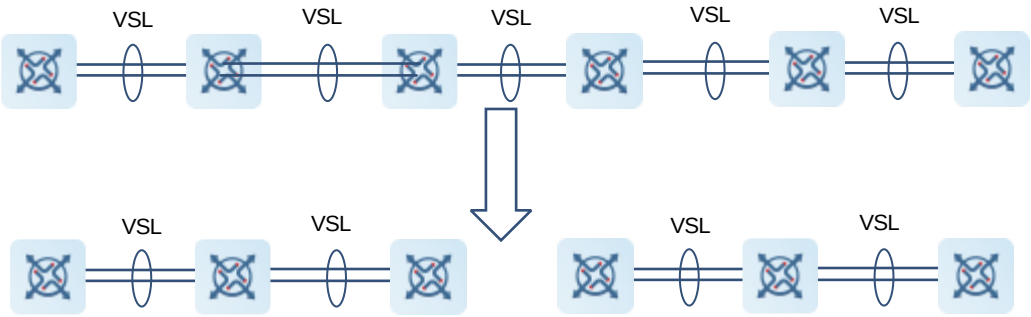
Note

The startup time varies with a device, and the first topology convergence time is different accordingly.

4. Topology splitting

The linear topology is split if the Virtual Switching Link-aggregation port (VSL-AP) link is disconnected. As shown in Figure 1-10, the VSU is split into two groups. In this case, there are two devices with the same configurations on the network, causing the network to malfunction. This topology splitting is resolved by deploying the dual-active detection (DAD) function (see section 1.1.4 DAD).

Figure 1-10 Topology Splitting



5. Topology combination

Topologies are combined when two VSUs with the same VSU domain ID are connected through a VSL-AP link. During topology combination, one of the VSUs automatically restarts in an attempt to join the other VSU, as shown in Figure 1-11.

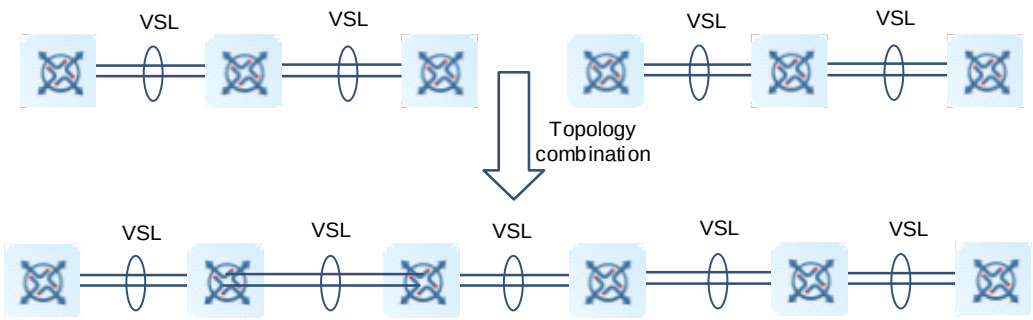
Topologies are combined based on the principle of minimizing the service impact caused by topology combination. The topology combination rules are as follows (topology combination starts from the first rule; if the optimal topology is not selected according to the first rule, the system goes on with the next rule for judgment):

(1) The user configurations are superior to other configurations. A VSU member device with the highest priority prevails.

(2) If the active device cannot be determined according to the preceding rule, a device with a smaller device ID prevails (in a case with two global active devices).

(3) If the active device cannot be determined according to the preceding rule, a device with a smaller MAC address prevails (in a case with two global active devices).

Figure 1-11 Topology Combination



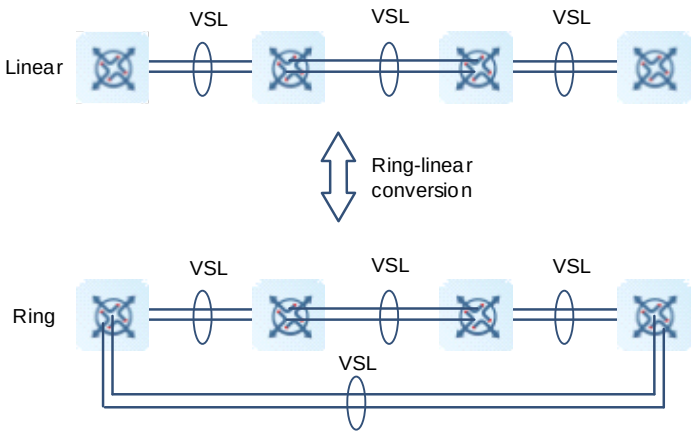
Note

During topology combination of two VSUs, they must be elected. The VSU that fails the election automatically restarts and joins the other VSU in hot mode.

6. Topology conversion

As shown in Figure 1-12, when one VSL-AP link is disconnected, the ring topology is converted into a linear one. The whole VSU can still run normally without network disconnection. However, to avoid the failure of other VSL-AP links or nodes, troubleshoot the VSL fault in time for VSL recovery. After the VSL-AP link is recovered, the linear topology is converted back into a ring one.

Figure 1-12 Conversion Between the Ring Topology and Linear Topology



1.1.4 DAD

When the VSL is disconnected, the standby device becomes the active device. If the original active device is still running, two active devices are main roles and an IP address conflict and other problems occur in the LAN due to their same configurations. In this case, the VSU must detect dual device devices, and take recovery measures. The VSU supports DAD in two ways:

- Bidirectional forwarding detection-based (BFD-based) DAD
- AP-based DAD

1. Detection rules

Determine the desired active device according to the following rules one by one:

(1) The healthier device prevails. (A greater sum of bandwidths of up physical ports excluding the administration port and VSL port indicates a healthier device).

(2) The global active device with a higher priority prevails.

(3) The global active device in the VSU with more physical devices prevails.

(4) The global active device with the smaller ID prevails.

(5) The global active device with the smaller MAC address prevails.

(6) The global active device with the longer startup time prevails.

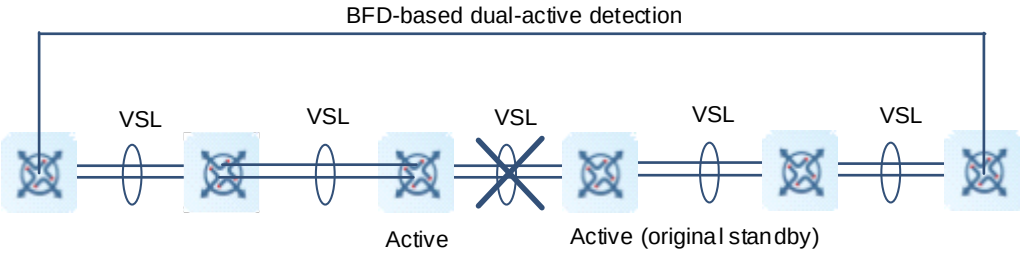
Caution

If DAD is not configured, the network is interrupted after the topology is split.

2. BFD-based DAD

The VSU supports the BFD-based DAD function. Figure 1-13 shows the connection topology. A dedicated link for DAD is added between two edge devices. When the VSL between the global active and standby devices is disconnected, two active devices coexist. If the BFD-based DAD function is configured, the two active devices send BFD-based DAD packets to each other through the BFD link, and find two identical active devices. Finally, the VSU including one of the active devices is shut down based on rules (see "Topology combination" for details) to enter the Recovery mode to avoid network exceptions.

Figure 1-13 BFD-based DAD



Caution

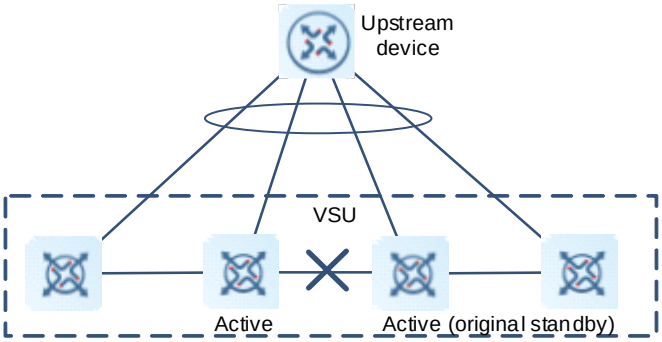
- When there is only one pair of BFD links, you are advised to deploy them at both ends of the topology.
- Extended BFD is used for the BFD-based detection, and the DAD ports cannot be configured by the existing BFD configurations and display commands.

3. AP-based DAD

The VSU also supports the AP-based DAD mechanism. Figure 1-14 shows the connection topology. The VSU and the upstream device must support the AP-based DAD function. When the VSL port is disconnected, dual active devices coexist and send detection packets to each AP member port. The upstream device forwards the detection packets from one active device to the other. The AP is composed of four member ports, which are

connected to different devices in the VSU. When the topology is split, the four member ports all send and receive detection packets, and find two identical active devices. Finally, the VSU including one of the active devices is shut down based on rules (see "Topology combination" for details) to enter the Recovery mode to avoid network exceptions.

Figure 1-14 AP-based DAD



Specification

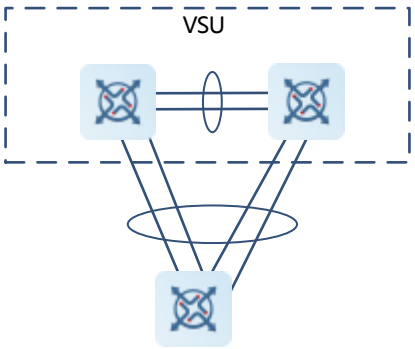
In the preceding topology, the upstream device must be a Ruijie device and can forward detection packets.

1.1.5 Traffic Forwarding

1. Cross-device Aggregation

An AP binds multiple physical links to form a logical link. The VSU supports an AP across member devices. As shown in Figure 1-15, two devices form a VSU and switch A is connected to the VSU as an AP. For switch A, the AP connections shown in the figure are equivalent to those of a common AP group.

Figure 1-15 Cross-device AP



A peripheral device is physically connected to each device in the VSU when a cross-device AP is configured. The advantages are as follows:

- Reserved bandwidth for the VSL: For cross-device AP traffic, the AP member of the same device is preferentially selected as the traffic egress, to avoid unnecessary traffic from being transmitted over the VSL.
- Improved network reliability: If a chassis fails, a member port on a normal device still works properly.

Table 1-1 lists the possible cross-device AP faults and their impact:

Table 1-1 Cross-device AP Faults and Principle Description

Fault Scenario		Principle Description
Link fault	A single link of the AP is faulty.	● The cross-device AP redistributes traffic among the remaining normal links. ● A VSL is needed to forward traffic whose egress port is a port on the device with the faulty link.
	All links of the AP are faulty.	● The AP state changes to link down just as a common AP is disconnected.
Device fault	The active device is faulty.	● The original standby device is switched to the active device. ● Member ports on other member devices continue to work properly ● The cross-device AP redistributes traffic among the remaining normal links.
	The standby/candidate device is faulty.	● The AP member ink connected to the member device is disconnected but other member links still work properly. ● The cross-device AP redistributes traffic among the remaining normal links.

2. Traffic balancing

In a VSU, traffic may have multiple egresses. The AP and Equal-cost Multi-path Routing (ECMP) have respective traffic balancing algorithms, for example, traffic is balanced based on the source and destination MAC addresses. For details, see the description about the link AP module in the interface configuration guide. In this configuration guide, packets received by the local device are preferentially forwarded by the local device. In this way, packets are forwarded to other devices not through a VSL.

1.1.6 System Management

1. Console access

The console of the VSU active device manages multiple devices in the system. The consoles of the standby and candidate devices do not support command line input. However, you can configure VSU-related commands on the active device for a specified member device, or log in to the console of the active device through the serial port of the standby device. You can also redirect to the master supervisor module of a device by running the **session** command.

2. Interface naming

In VSU mode, the same slot ID may appear on multiple devices. Therefore, device ID (switch ID) is added to an interface name. For example, interface GigabitEthernet 1/1/1 indicates GE port 1 in slot 0 of a device with the ID of 1; interface GigabitEthernet 2/1/2 indicates GE port 2 in slot 0 of a device with the ID of 2.

3. Access to the file system

In VSU mode, you can access to the file systems on other member devices from the active device. The detailed access method is the same as that of the local file system. The only difference lies in URL prefixes.

4. Log management

All member devices of the VSU can display syslogs. Syslogs generated by the active device are displayed on the console of the active device, and their format is identical to that of syslogs displayed in standalone mode. Syslogs of other member devices are also displayed on the console of the active device, but their format is different from that of syslogs in standalone mode, because the device ID is added to the syslogs. For example, a syslog generated in standalone mode is "%VSU-5-DTM_TOPO_CVG: Node discovery done. Topology converged." Accordingly, a syslog generated by a member device with the device ID of 3 is "%VSU-5-DTM_TOPO_CVG:(3) Node discovery done. Topology converged."

1.1.7 System Upgrade

Usually, the main program versions of member devices in the VSU need to be consistent. But if such numerous member devices are upgraded one by one in standalone mode, this consumes much time and effort, and easily causes errors. The VSU offers a comprehensive system upgrade solution below:

- Check the main program versions of all member devices to determine whether the versions are consistent.
- If inconsistency is identified, the VSU synchronizes the main program of the active device to all member devices via Trivial File Transfer Protocol.

1.1.8 Quick Blinking Location

In the network cabling environment, the equipment room and the operating console are often in different places. If there are many devices in the environment, network administrators are hard to locate specific devices. Quick blinking location provides network administrators with a method for locating devices by quick blinking. By enabling this function for a device on the console, you easily find the corresponding device in the equipment room.

Note

A state of the original Status indicator is not displayed when quick blinking location is enabled, and is displayed only when it is disabled.

1.2 Restrictions and Guidelines

- A VSU can be set up by different products of the same series, but not by products of different series.
- Use 10G ports or above as the VSL ports.
- When the Switched Port Analyzer (SPAN) function is configured, a VSL port is used as neither the source port nor the destination port of SPAN.

1.3 Configuration Task Summary

The VSU configuration includes the following tasks:

(1) Setting Up a VSU

(2) Configuring BFD-based DAD

(3) Configuring AP-based DAD

(4) Configuring the VSL

(5) (Optional) Configuring VSU Attributes

All the following configuration tasks are optional and may be selected as needed.

- Configuring Basic VSU Attributes
- Configuring Traffic Balancing
- Switching to Standalone Mode
- Configuring Recovery Method for Recovery Mode

(6) (Optional) Configuring Quick Blinking Location

1.4 Setting Up a VSU

1.4.1 Overview

Devices start up in standalone mode by default. You need to configure the same domain ID on all devices used to set up a VSU, and assign a unique virtual machine ID for each device.

1.4.2 Restrictions and Guidelines

- If the current device works in VSU mode and cannot directly switch to another VSU domain, first switch to standalone mode and then to another VSU.
- The VSU configurations are applicable to a single physical device, and the configurations are stored in the special configuration file **config_vsu.dat**. Therefore, the **show running config** command does not display the VSU configurations. You can display the current VSU configurations by running the **show switch virtual config** command only.
- In standalone mode, the VSU running information is blank. When you run the **show switch virtual**, a prompt is displayed, indicating that the device works in standalone mode and there is no VSU running information.

1.4.3 Prerequisites

The VSL between VSU devices is normal.

1.4.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the VSU domain ID and enter the config-vs-domain configuration mode.

switch virtual domain *domain-id*

The default domain ID is 100.

Only devices with the same domain ID can form a VSU.

(4) Configure the device ID of the VSU.

switch *switch-id*

The default device ID is 1.

(5) (Optional) Configure the device priority.

switch *switch-id* **priority** *priority-number*

The default device priority is 100. A larger value indicates a higher priority.

(6) (Optional) Configure the device alias.

switch *switch-id* **description** *device-name*

No device alias is configured by default.

(7) (Optional) Specify the manner of saving the VSU configuration file of a device.

switch cfg_mode { **normal** | **single** }

normal is selected by default. That is, the VSU configurations are separately saved in **config_vsu.dat**.

(8) Return to the global configuration mode.

exit

(9) Enter the VSL port configuration mode.

vsl-port

(10) Add the member ports to the VSL.

port-member interface *interface-type interface-number*

No member port is configured by default.

The VSL member port is a two-dimensional port in standalone mode. The port must be a 10G port or above.

(11) Return to the privileged EXEC mode.

end

(12) Switch the device from the standalone mode to the VSU mode.

switch convert mode virtual

A device works in standalone mode by default.

1.5 Configuring BFD-based DAD

1.5.1 Overview

The BFD-based DAD is configured to prevent coexistence of two active devices.

1.5.2 Restrictions and Guidelines

- BFD detection ports must be direct physical routed ports in different devices.

- The configured port type is unlimited. DAD links are used to transmit only BFD packets and thus need less traffic. Therefore, you are advised to configure a 1000M or 100M port as the DAD port.
- After a layer-3 (L3) routed port configured for DAD is switched to a layer-2 (L2) switching port (by running the **switchport** command on the port), the BFD DAD configuration is automatically cleared.
- You are advised to directly connect only the active and standby devices in BFD mode.
- When the VSUs detect a dual-active conflict and one VSU enters the **Recovery** mode, you can rectify the fault by eliminating the VSL failure rather than by directly resetting the VSU in the **Recovery** mode. Otherwise, a dual-active conflict may be incurred in the network.
- Excluded ports in **Recovery** mode must be routed ports rather than VSL ports. After an excluded port is switched from a routed port to a switching port (by running the **switchport** command on the port), the excluded port configuration associated with this port is automatically cleared.
- When dual active devices are detected, one of them must enter the **Recovery** mode. In **Recovery** mode, all service ports of the device must be disabled. To ensure normal use of certain special ports (for example, management ports for remote login to devices), you can configure excluded ports that are not disabled in Recovery mode.

1.5.3 Prerequisites

A VSU has been set up.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the BFD detection port configuration mode.

interface *interface-type interface-number*

(4) Configure the BFD detection port as a routed port.

no switchport

A port is an L2 switching port by default.

(5) Return to the global configuration mode.

exit

(6) Enter the VSU domain configuration mode.

switch virtual domain *domain-id*

(7) Enable the DAD function and specify the BFD-based detection method.

dual-active detection bfd

The DAD function is disabled by default.

(8) Configure a BFD detection port.

dual-active bfd interface *interface-type interface-number*

No BFD detection port is configured by default.

(9) (Optional) Configure the list of excluded ports for Recovery mode.

dual-active exclude interface *interface-type interface-number*

No excluded port is configured by default.

1.6 Configuring AP-based DAD

1.6.1 Overview

The AP-based DAD method is configured to prevent coexistence of two active devices.

1.6.2 Restrictions and Guidelines

- When the VSUs detect a dual-active conflict and one VSU enters the **Recovery** mode, you can rectify the fault by eliminating the VSL failure rather than by directly resetting the VSU in the **Recovery** mode. Otherwise, a dual-active conflict may be incurred in the network.
- Excluded ports for the **Recovery** mode must be routed ports rather than VSL ports. After an excluded port is switched from a routed port to a switching port (by running the **switchport** command on the port), the excluded port configuration associated with this port is automatically cleared.

1.6.3 Prerequisites

A VSU has been set up.

1.6.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VSU domain configuration mode.

switch virtual domain *domain-id*

(4) Enable the DAD function and specify the AP-based detection method.

dual-active detection aggregateport

The DAD function is disabled by default.

(5) Configure an AP-based detection port.

dual-active interface *interface-type interface-number* [**vlan** *vlan-id*]

No AP-based detection port is configured by default.

When the AP is a trunk port and the native VLAN is beyond the VLAN range allowed by the AP-based detection port, configure a detection VLAN for the AP-based detection port. The configured VLAN must fall in the VLAN range allowed by the trunk port, and be created on the device in advance.

(6) In AP mode of the upstream and downstream devices, enable the function of forwarding AP-based DAD packets.

dad relay enable

The DAD packets are not forwarded by default.

(7) (Optional) Configure the list of excluded ports for Recovery mode.

dual-active exclude interface *interface-type interface-number*

No excluded port is configured by default.

When dual active devices are detected, one of them must enter the **Recovery** mode. In **Recovery** mode, all service ports of the device must be disabled. To ensure normal use of certain special ports (for example, management ports for remote login to devices), you can configure excluded ports that are not disabled in **Recovery** mode.

1.7 Configuring the VSL

1.7.1 Overview

To modify a VSL member port (switch to or back from a common port, or add or delete a VSL) during setup or running of a VSU, you can log in to the VSU console through a serial port or Telnet.

1.7.2 Restrictions and Guidelines

- In practice, dynamic negotiation is used by the VSL AP to prevent link connection faults. A VSL port pool is first configured, and all VSL ports of the same member device are added to the same AP after negotiation. Ports connected to the same device are in the same AP.
- During VSU running, configured VSL member links take effect immediately. VSL ports need to be configured on all devices.
- Chassis-type devices allow 10G SFP ports or ports with higher bandwidth to act as VSL ports. Box-type devices depend on the actual product version.
- Do not set member ports (four 10G ports) of a 40G port as VSL member ports.
- To prevent a loop from being instantaneously generated when a VSL member port exits the VSL AP, the system automatically sets the member port to the **shutdown** state when you run the configuration command. After the VSL member port exits the VSL AP, you can reconnect the link and run the **no shutdown** command to enable the port again. When you configure the VSL port, the system runs the **shutdown** command to shut down the port first. If the configuration fails and you need to continue using the port as a common port, you can run the **no shutdown** command to enable the port again. An added member port ID must be three-dimensional.
- If a port is configured as an NLB reflex port, this port can be switched to a VSL member port only after the NLB reflex port configuration is deleted.
- If the VSU topology is split when a VSL port is switched to a common port, the VSL port must not be deleted. You can disconnect the physical port before deleting the VSL port.

1.7.3 Prerequisites

A VSU has been set up.

1.7.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VSL port configuration mode.

vsl-port

(4) Add the member ports for the VSL.

port-member interface *interface-type interface-number*

No VSL member port is configured by default.

The VSL member port must be a 10G port.

1.8 Configuring VSU Attributes

1.8.1 Overview

In VSU mode, you can configure enhancements to increase the reliability and usability of the VSU.

1.8.2 Configuration Tasks

The VSU attribute configuration includes the following tasks:

All the following configuration tasks are optional and may be selected as needed.

- Configuring Basic VSU Attributes
- Configuring the VSL
- Configuring Traffic Balancing
- Switching to Standalone Mode
- Configuring Recovery Method for Recovery Mode

1.8.3 Configuring Basic VSU Attributes

1. Overview

During VSU setup or running, you can log in to the console of the active or standby device of the VSU to modify some parameters.

2. Restrictions and Guidelines

All configuration commands take effect only after the device is restarted, except the device alias modification command, which takes effect immediately.

3. Prerequisites

A VSU has been set up.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VSU domain configuration mode.

switch virtual domain *domain-id*

(4) Configure the basic VSU attributes as required.

- Modify the VSU domain ID of a specified device.

  switch *switch-id* **domain** *new-domain-id*

  The default VSU domain ID is 100.

- Modify the ID of the specified device.

  switch *switch-id* **renumber** *new-switch-id* [**force**]

  The default device ID is 1.

- Modify the priority of the specified device.

  switch *switch-id* **priority** *priority-number*

  The default device priority is 100.

- Modify the alias of the specified device.

  switch *switch-id* **description** *device-name*

  No device alias is configured by default.

- Set the CRC error parameter.

  switch crc errors *error-number* **times** *time-number*

  By default, one CRC error occurrence is recorded if the number of CRC errors incremented between two checks is 3 or more. If 10 consecutive CRC error occurrences is recorded, the port is considered abnormal.

- Specify the manner of saving the VSU configuration file of a device.

  switch cfg_mode { **normal** | **single** }

  normal is selected by default. That is, the VSU configurations are separately saved in **config_vsu.dat**.

1.8.4 Configuring Traffic Balancing

1. Overview

In the VSU, if egresses are distributed on multiple devices, traffic balancing allows forwarding traffic preferentially on the local device.

2. Restrictions and Guidelines

- By default, AP-based and ECMP-based Local Forward First (LFF) are enabled.
- In VSU mode, the cross-device AP-based LFF and ECMP-based LFF over routed ports are enabled by default. To set up a VSU with L3 switches, you are advised to configure the AP-based load balancing based on IP addresses (**src-ip**, **dst-ip**, and **src-dst-ip**).

3. Prerequisites

A VSU has been set up.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VSU domain configuration mode.

switch virtual domain *domain-id*

(4) Disable the AP-based LFF.

no switch virtual aggregateport-lff enable

In VSU mode, the AP-based LFF is enabled by default.

(5) Disable the ECMP-based LFF.

no switch virtual ecmp-lff enable

In VSU mode, the ECMP-based LFF is enabled by default.

1.8.5 Switching to Standalone Mode

1. Overview

This function switches devices in a VSU to the standalone mode.

2. Restrictions and Guidelines

You can switch devices in a VSU to the standalone mode by using a saved standalone configuration file, or by clearing the VSU configuration.

3. Prerequisites

A VSU has been set up.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Switch a device to the standalone mode.

switch convert mode standalone [*switch-id*]

A device works in standalone mode by default.

1.8.6 Configuring Recovery Method for Recovery Mode

1. Overview

This function disables the automatic restart function for the Recovery mode.

2. Restrictions and Guidelines

If the automatic restart function is disabled, you must enable this function again or manually restart the device to recover the device in recovery mode.

3. Prerequisites

A VSU has been set up.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VSU domain configuration mode.

switch virtual domain *domain-id*

(4) Disable the automatic restart function for the **Recovery** mode.

no recovery auto-restart enable

By default, the automatic restart function is enabled for the Recovery mode after the link fault is rectified.

1.9 Configuring Quick Blinking Location

1.9.1 Overview

When quick blinking location is enabled, the device status indicator blinks quickly.

1.9.2 Restrictions and Guidelines

- Quick blinking location is automatically disabled 30 minutes after it is started.
- The configuration takes effect immediately and cannot be saved. If you restart the device or perform an active/standby switch, quick blinking location is disabled.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enable/Disable quick blinking location.

led-blink { **enable** | **disable** } [**device** *switch-id*]

Quick blinking location is disabled by default. If no device ID is specified, the command applies to all devices in the VSU domain.

1.10 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-2 VSU Monitoring

Command	Purpose
show switch virtual [**topology** | **config** | **role balance**]	Views the topology, configurations, roles, and forwarding and balancing policies of the running VSU.
show switch virtual dual-active { **bfd** | **aggregateport** | **summary** }	Displays the information about the current DAD.
show switch virtual link [**port**]	Displays the information about the current VSL.
show switch id	Displays the ID of the current device.

1.11 Configuration Examples

1.11.1 Setting Up a VSU

1. Requirements

As shown in Figure 1-16, connect Device A to Device B through two 10G cables to form a VSU with basic configurations.

2. Topology

Figure 1-16 Topology of the VSU

3. Notes

- Configure the domain ID, device ID, device priority, device name, and VSL ports for the VSU.
- Configure the VSU switching mode.

4. Procedure

(1) On Device A, set the domain ID to 100, device ID to 1, device priority to 200, VSU device name to Device A, and VSL ports to tenGigabitEthernet 1/1 and tenGigabitEthernet 1/2.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# switch virtual domain 100
DeviceA(config-vs-domain)# switch 1
DeviceA(config-vs-domain)# switch 1 priority 200
DeviceA(config-vs-domain)# switch 1 description DeviceA
DeviceA(config-vs-domain)# switch crc errors 10 times 20
DeviceA(config-vs-domain))# exit
DeviceA(config)# vsl-port
DeviceA(config-vsl-port)# port-member interface tengigabitethernet 1/1
DeviceA(config-vsl-port)# port-member interface tengigabitethernet 1/2
DeviceA(config)# exit
DeviceA# switch convert mode virtual
```

(2) On Device B, set the domain ID to 100, device ID to 2, device priority to 100, VSU device name to Device B, and VSL ports to tenGigabitEthernet 1/1 and tenGigabitEthernet 1/2.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# switch virtual domain 100
DeviceB(config-vs-domain)# switch 2
DeviceB(config-vs-domain)# switch 2 priority 100
DeviceB(config-vs-domain)# switch 2 description DeviceB
DeviceB(config-vs-domain)# switch crc errors 10 times 20
DeviceB(config-vs-domain))# exit
DeviceB(config)# vsl-port
```

```
DeviceB(config-vsl-port)# port-member interface Tengigabitethernet 1/1
DeviceB(config-vsl-port)# port-member interface Tengigabitethernet 1/2
DeviceB(config-vsl-port)# exit
DeviceB# switch convert mode virtual
```

5. Verification

(1) Run the **show switch virtual role** command to verify whether the role of Device A is **Active** and that of Device B is **Standby**. If yes, the VSU is set up; if not, the VSU fails to be set up.

```
DeviceA# show switch virtual role
Switch_id    Domain_id    Priority    Position    Status    Role
Description
1(1)        100(100)     200(200)    LOCAL       OK        ACTIVE       DeviceA
2(2)        100(100)     100(100)    REMOTE      OK        STANDBY      DeviceB
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
switch virtual domain 100
!
switch 1
switch 1 priority 200
switch 1 description DeviceA
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!
end
```

- Device B configuration file

```
hostname DeviceB
!
switch virtual domain 100
!
switch 2
switch 2 priority 100
switch 2 description DeviceB
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!
```

```
end
```

7. Common Errors

- Different domain IDs (**domain-id**) are configured.
- The VSL ports are not up.

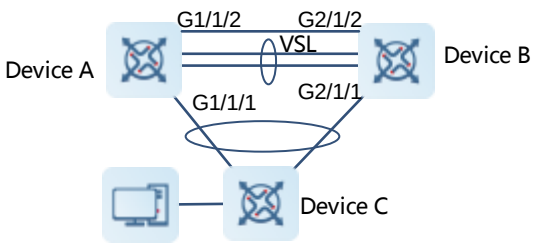
1.11.2 Configuring BFD-based DAD

1. Requirements

As shown in Figure 1-17, form a VSU with Device A and Device B. To prevent an IP address conflict in the LAN caused by two identical active devices in case of VSL disconnection, configure the BFD-based detection mechanism to quickly detect two active devices and to actively switch one of them to the Recovery mode (the service forwarding function is disabled).

2. Topology

Figure 1-17 Topology for BFD-based DAD



3. Notes

- Enable the BFD-based DAD.
- Designate a BFD detection port, which must be configured as a routed port.

Note

As Device A and Device B form the VSU, the preceding configuration can be performed on either Device A or Device B. Device A is used as an example.

4. Procedure

On Device A, configure GigabitEthernet 1/1/2 and GigabitEthernet 2/1/2 as routed ports, enable the BFD-based DAD, and set the BFD-based detection ports to GigabitEthernet 1/1/2 and GigabitEthernet 2/1/2.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 1/1/2
DeviceA(config-if-GigabitEthernet 1/1/2)# no switchport
DeviceA(config)# interface GigabitEthernet 2/1/2
DeviceA(config-if-GigabitEthernet 2/1/2)# no switchport
DeviceA(config-if)# switch virtual domain 1
DeviceA(c config-vs-domain)# dual-active detection bfd
DeviceA(config-vs-domain)# dual-active bfd interface GigabitEthernet 1/1/2
```

```
DeviceA(config-vs-domain)# dual-active bfd interface GigabitEthernet 2/1/2
```

5. Verification

Disconnect all VSLs, log in to the console of Device A , and run the **show switch virtual** command to check whether **Status** is set to **OK** (Device A runs normally when dual active devices are detected).

```
VSU# show switch virtual
Switch_id    Domain_id    Priority    Position    Status    Role
Description
--------------------------------------------------------------------------------
---------
1(1)         1(1)         100(100)    LOCAL       OK        ACTIVE       DeviceA
```

Log in to the console of Device A, and run the **show switch virtual dual-active bfd** command to check whether the BFD enabling status is **Yes** and the status of the BFD-based detection port GigabitEthernet 2/1/2 of Device B is **Down**.

```
VSU-RECOVERY-2# show switch virtual dual-active bfd
BFD dual-active detection enabled: Yes
BFD dual-active interface configured:
  GigabitEthernet 1/1/2: UP
  GigabitEthernet 2/1/2: DOWN
```

Log in to the console of Device B, and run the **show switch virtual** command to check whether the value of **Status** changes to **Recovery** and the device name is suffixed with **-RECOVERY-2**.

```
VSU-RECOVERY-2#show switch virtual
Switch_id    Domain_id    Priority    Position    Status    Role
Description
--------------------------------------------------------------------------------
----------
2(2)         1(1)          90(90)     LOCAL       Recovery  ACTIVE       DeviceB
```

Log in to the console of Device B, and run the **show switch virtual dual-active summary** command to check whether the value of **In dual-active recovery mode** is **Yes** (Device B works in recovery mode).

```
VSU-RECOVERY-2# show switch virtual dual-active summary
BFD dual-active detection enabled: Yes
Aggregateport dual-active detection enabled: No
Interfaces excluded from shutdown in recovery mode:
In dual-active recovery mode: Yes
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 1/1/2
 no switchport
!
interface GigabitEthernet 2/1/2
 no switchport
!
```

```
switch virtual domain 1
dual-active detection bfd
dual-active bfd interface GigabitEthernet 1/1/2
dual-active bfd interface GigabitEthernet 2/1/2
!
switch 1
switch 1 priority 100
switch 1 description DeviceA
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!

end
```

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 1/1/2
 no switchport
!
interface GigabitEthernet 2/1/2
 no switchport
!
switch virtual domain 1
dual-active detection bfd
dual-active bfd interface GigabitEthernet 1/1/2
dual-active bfd interface GigabitEthernet 2/1/2
!
switch 2
switch 2 priority 90
switch 2 description DeviceB
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!

end
```

7. Common Errors

- The BFD-based detection port is not configured as a routed port.

- Either BFD-based or AP-based DAD is selected.

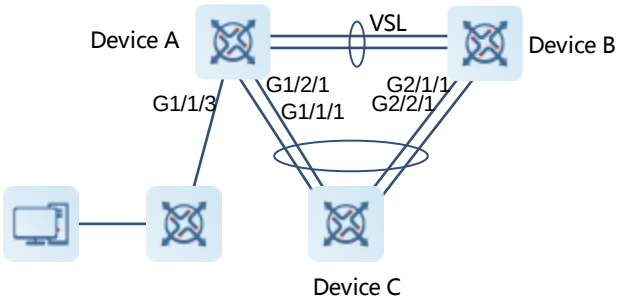
1.11.3 Configuring AP-based DAD

1. Requirements

As shown in Figure 1-18, form a VSU with Device A and Device B, and connect Device C to Device A and Device B separately over an AP. To prevent an IP address conflict in the LAN caused by two identical active devices in case of VSL disconnection, configure the AP-based detection mechanism to quickly detect two active devices and to actively switch one of them to the Recovery mode (the service forwarding function is disabled).

2. Topology

Figure 1-18 Topology for AP-based DAD



3. Notes

- Configure the ports connecting Device C to Device A and Device C to Device B as the same AP group.
- Enable the AP-based DAD.
- Configure the AP-based detection port.
- Configure the ports connecting Device C to Device A and Device B as the same AP group. Enable the function of forwarding AP-based DAD packets of this port group.

Note

As Device A and Device B form the VSU, the preceding configuration can be performed on either Device A or Device B. Device A is used as an example.

4. Procedure

On Device A, add GigabitEthernet 1/1/1, GigabitEthernet 1/2/1, GigabitEthernet 2/1/1, and GigabitEthernet 2/2/1 to the AP group port-group 1.

```
DeviceA> enable
DeviceA# configure
DeviceA(config)# interface range GigabitEthernet 1/1/1-2
DeviceA(config-if-range)# port-group 1
DeviceA(config-if-range)# interface range GigabitEthernet 2/1/1-2
DeviceA(config-if-range)# port-group 1
```

On Device A, enable the AP-based DAD, and set the detection port to aggregatePort 1.

```
DeviceA> enable
DeviceA# configure
DeviceA(config)# switch virtual domain 1
DeviceA(config-vs-domain)# dual-active detection aggregateport
DeviceA(config-vs-domain)# dual-active interface aggregatePort 1
```

On Device C, add GigabitEthernet 0/1, GigabitEthernet 0/2, GigabitEthernet 0/3, and GigabitEthernet 0/4 to the AP group port-group 1.

```
DeviceC> enable
DeviceC# configure
DeviceC(config)# interface range GigabitEthernet 0/1-4
DeviceC(config-if-range)# port-group 1
```

On Device C, configure the function of forwarding DAD packets.

```
DeviceC> enable
DeviceC# interface aggregatePort 1
DeviceC(config-if-AggregatePort 1)# dad relay enable
```

5. Verification

Run the **show switch virtual dual-active summary** and **show switch virtual dual-active aggregateport** commands to check whether the configurations are correct.

```
DeviceA# show switch virtual dual-active summary
Aggregateport dual-active detection enabled: Yes
Interfaces excluded from shutdown in recovery mode:
In dual-active recovery mode: NO
DeviceA# show switch virtual dual-active aggregateport
Aggregateport dual-active detection enabled: Yes
Aggregateport dual-active interface configured:
  AggregatePort 1: UP
    GigabitEthernet 1/1/1: UP
    GigabitEthernet 1/2/1: UP
    GigabitEthernet 2/1/1: UP
    GigabitEthernet 2/2/1: UP
```

```
Hostname_VSU-RECOVERY-2#sh switch virtual dual-active su
BFD dual-active detection enabled: No
Aggregateport dual-active detection enabled: Yes
Interfaces excluded from shutdown in recovery mode:
In dual-active recovery mode: Yes
Hostname_VSU-RECOVERY-2#sh switch virtual
Switch_id    Domain_id    Priority    Position    Status    Role
Description
-------------------------------------------------------------------------------
---------
2(2)        100(100)     100(100)    LOCAL       Recovery   ACTIVE       CS86-207
Hostname_VSU-RECOVERY-2#show switch virtual dual-active aggregateport
Aggregateport dual-active detection enabled: Yes
```

```
Aggregateport dual-active interface configured:
  AggregatePort 7: DOWN
    GigabitEthernet 1/0/1: DOWN
    GigabitEthernet 2/0/1: DOWN
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 1/1/1
 port-group 1
!
interface GigabitEthernet 1/1/2
 port-group 1
!
interface GigabitEthernet 2/1/1
 port-group 1
!
interface GigabitEthernet 2/1/2
 port-group 1
!
switch virtual domain 1
dual-active detection aggregateport
dual-active interface aggregatePort 1
!
switch 1
switch 1 priority 100
switch 1 description DeviceA
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!

end
```

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 1/1/1
 port-group 1
!
interface GigabitEthernet 1/1/2
 port-group 1
!
```

```
interface GigabitEthernet 2/1/1
 port-group 1
!
interface GigabitEthernet 2/1/2
 port-group 1
!
switch virtual domain 1
dual-active detection aggregateport
dual-active interface aggregatePort 1
!
switch 2
switch 2 priority 90
switch 2 description DeviceB
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!

end
```

- Device C configuration file

```
hostname DeviceC
!
interface GigabitEthernet 0/1
 port-group 1
!
interface GigabitEthernet 0/2
 port-group 1
!
interface GigabitEthernet 0/3
 port-group 1
!
interface GigabitEthernet 0/4
 port-group 1
!
interface AggregatePort 1
 dad relay enable
!

end
```

7. Common Errors

- The AP detection port must be an AP.
- Either AP-based or BFD-based DAD is selected.

1.12 Common Misconfigurations

- The VSL port type is not supported.
- Different domain IDs (**domain-id**) are configured.

Interface Configuration

1. Ethernet Interface Configuration
2. Aggregate Port Configuration

Contents

1 Configuring Ethernet Interface 1
1.1 Introduction 1
1.1.1 Basic Concepts 1
1.1.2 Interface Configuration 3
1.1.3 Interface Description and Administrative Status 4
1.1.4 MTU of an Interface 5
1.1.5 Configuring Bandwidth of an Interface 5
1.1.6 Configuring Carrier Delay 5
1.1.7 Link Trap Policy 5
1.1.8 Interface Index Persistence 5
1.1.9 Configuring Routed Port 5
1.1.10 Configuring L3 AP 6
1.1.11 Configuring Basic Attributes of Interfaces 6
1.1.12 Automatic Module Detection 7
1.1.13 Protected Port 8
1.1.14 Port Errdisable Recovery 8
1.1.15 Optical Module Alarm Detection 8
1.1.16 Optical Module Antifake Detection 9
1.1.17 Splitting and Combination of 40G/100G Interfaces 9
1.1.18 Configuring Interface Traffic Statistics 9
1.1.19 EEE 9
1.1.20 Port Flapping Protection 10

1.1.21 Interface Syslog 10

1.1.22 Configuring the MAC Address of an Interface 10

1.1.23 VLAN Encapsulation Flag on Interfaces 11

1.1.24 Configuring the FEC Mode of an Interface 11

1.1.25 Configuring the Sampling Period of Ethernet Interface Statistics 11

1.1.26 Configuring Enhanced Name Display for Interfaces 12

1.1.27 Including Interframe Gaps in Interface Packet Rate Statistics 12

1.2 Configuration Task Summary 12

1.3 Configuring Basic Features 12

1.3.1 Overview 12

1.3.2 Restrictions and Guidelines 12

1.3.3 Procedure 13

1.4 Configuring Interface Attributes 14

1.4.1 Overview 14

1.4.2 Restrictions and Guidelines 14

1.4.3 Procedure 14

1.5 Monitoring 16

1.6 Configuration Examples 19

1.6.1 Configuring Interface Attributes 19

1.6.2 Configuring Interconnection Interfaces 22

1 Configuring Ethernet Interface

1.1 Introduction

Interfaces are important in implementing data switching on network devices. Ruijie devices support two types of interfaces: physical ports and logical interfaces. A physical port is a hardware port on a device, such as the 100M Ethernet interface and Gigabit Ethernet interface. A logical interface, such as the loopback interface and tunnel interface, can be associated with a physical port or independent of any physical port. For network protocols, physical ports and logical interfaces are processed in the same way.

1.1.1 Basic Concepts

1. Interface Classification

Interfaces on Ruijie devices fall into two categories:

- L2 interface (Switch or bridge mode)
- L3 interface (supported by L3 devices)

Common L2 interfaces are classified into the following types:

- Switch port
- L2 aggregate port (AP)

Common L3 interfaces are classified into the following types:

- Routed port
- L3 AP
- Switch virtual interface (SVI)
- Loopback interface
- Tunnel interface

2. Switch Port

A switch port is a single physical port on the device, and implements only the L2 switching function. The switch port is used to manage physical ports and L2 protocols related to physical ports.

3. L2 AP

An AP is formed by aggregating multiple physical ports. Multiple physical links can be bound together to form a simple logical link. This logical link is called an AP.

For L2 switching, an AP is equivalent to a switch port that combines bandwidths of multiple ports, thus expanding the link bandwidth. Frames sent over the L2 AP are balanced among the L2 AP member ports. If one member link fails, the L2 AP automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

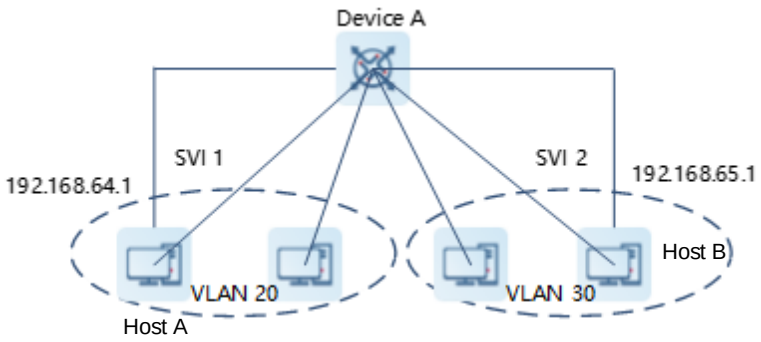
4. SVI

The SVI can be used as the management interface of the local device, through which the administrator can manage the device. You can also create an SVI as a gateway interface, which is mapped to the virtual interface

of each virtual local area network (VLAN) to implement routing across VLANs among L3 devices. You can run the **interface vlan** command to create an SVI and assign an IP address to this interface to set up a route between VLANs.

As shown in Figure 1-1, the hosts in VLAN 20 can directly communicate with each other without participation of L3 devices. If Host A in VLAN 20 wants to communicate with Host B in VLAN 30, SVI 1 of VLAN 20 and SVI 2 of VLAN 30 must be used.

Figure 1-1 Schematic Diagram of SVI



5. Routed Port

A physical port on a L3 device can be configured as a routed port, which functions as the gateway interface for L3 switching. A routed port is unrelated with a specific VLAN. Instead, it just serves as an access port. The routed port cannot be used for L2 switching.

You can run the **no switchport** command to change a switch port to a routed port and assign an IP address to this port to set up a route. Note that all L2 features of the switch port will be deleted after you run the **no switchport** command.

Note

If a port is a L2 AP member port or a DOT1X port that is not authenticated, you cannot run the **switchport** or **no switchport** command to configure the switch port or routed port.

6. L3 AP

Like the L2 AP, a L3 AP is a logical port that aggregates multiple physical member ports. The aggregated ports must be the L3 ports of the same type. The AP functions as a gateway interface for L3 switching. Multiple physical links are combined into one logical link, expanding the bandwidth of a link. Frames sent over the L3 AP are balanced among the L3 AP member ports. If one member link fails, the L3 AP automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

A L3 AP cannot be used for L2 switching. You can run the **no switchport** command to change a L2 AP that does not contain any member port into a L3 AP, add multiple routed ports to this L3 AP, and then assign an IP address to this L3 AP to set up a route.

7. Loopback Interface

The loopback interface is a local L3 logical interface simulated by the software that is always **Up**. Packets sent to the loopback interface are processed on the device locally, including the route information. The IP address of the loopback interface can be used as the device ID of the Open Shortest Path First (OSPF) routing protocol, or as both the local address of telnet and the remote telnet access address. The procedure for configuring a loopback interface is similar to that for configuring an Ethernet interface. You can treat the loopback interface as a virtual Ethernet interface.

8. Tunnel Interface

The Tunnel interface implements the tunnel function. Over the Tunnel interface, transmission protocols (e.g., IP) can be used to transmit packets of any protocol. Like other logical interfaces, the tunnel interface is also a virtual interface of the system. Instead of specifying any transmission protocol or load protocol, the tunnel interface provides a standard point-to-point (P2P) transmission mode. Therefore, a tunnel interface must be configured for every single link.

1.1.2 Interface Configuration

You can run the **interface** command in the global configuration mode to enter the interface configuration mode. You can configure interface-related attributes in interface configuration mode.

If you enter the interface configuration mode of a non-existing logical interface, the interface will be created. You can also run the **interface range** or **interface range macro** command in the global configuration mode to configure the range (IDs) of interfaces. Interfaces defined in the same range must be of the same type and have the same features.

You can run the **no interface** command in global configuration mode to delete a specified logical interface.

1. Interface Numbering Rules

In stand-alone mode, the interface ID corresponding to a physical port consists of two parts: slot ID and port ID on the slot. For example, if the slot ID of the port is 2, and port ID on the slot is 3, the interface ID is 2/3. In virtual switch unit (VSU) mode or stack mode, the interface ID corresponding to a physical port consists of three parts: device ID, slot ID, and port ID on the slot. For example, if the device ID is 1, slot ID is 2, and port ID on the slot is 3, the interface ID is 1/2/3.

The device ID ranges from 1 to the maximum number of member devices supported.

The slot number rules are as follows: The static slot ID is 0, whereas the ID of a dynamic slot (pluggable module or line card) ranges from 1 to the number of slots. Assume that you are facing the device panel. Dynamic slots are numbered from 1 sequentially from front to rear, from left to right, and from top to bottom.

The ID of a port on the slot ranges from 1 to the number of ports on the slot, and is numbered sequentially from left to right.

You can select fiber or copper as the medium of a combo port. Regardless of the medium selected, the combo port uses the same port ID.

The ID of an AP ranges from 1 to the number of APs supported by the device.

The ID of an SVI is the ID of the VLAN corresponding to this SVI.

2. Configuring Interfaces Within a Range

You can run the **interface range** command in the global configuration mode to configure multiple interfaces at a time. Attributes configured in the **interface range** mode apply to all these interfaces.

The **interface range** command can be used to specify several range segments, and each range segment can be separated using a comma (,). The types of interfaces within all ranges specified in a command must be the same. The **macro** parameter is used to configure the macro corresponding to a range. For details, see "Configuring Macros of Interface Ranges".

When the **interface range** command is used, the parameter formats vary with different interface types. The common valid interface range formats are as follows:

- **FastEthernet** device/slot/{ start-port } - { end-port }.
- **GigabitEthernet** device/slot/{ start-port } - { end-port }.
- **TenGigabitEthernet** device/slot/{ start-port } - { end-port }.
- **FortyGigabitEthernet** device/slot/{ start-port } - { end-port }.
- **AggregatePort** { start-port } - { end-port }. The value range is from 1 to the maximum number of APs supported by the device.
- **vlan** vlan-ID-vlan-ID. The value range of VLAN ID is from 1 to 4094.
- **Loopback** loopback-start-ID-loopback-end-ID. The value range is from 1 to 2147483647.
- **Tunnel** tunnel-start-ID-tunnel-end-ID. The value range is from 0 to the maximum number of tunnel interfaces supported by the device minus 1.

3. Configuring Macros of Interface Ranges

You can define some macros to replace the interface ranges. Before using the **macro** parameter in the **interface range** command, you must first run the **define interface-range** command in the global configuration mode to define these macros.

In addition, you can run the **no define interface-range** *macro-name* command in the global configuration mode to delete the configured macros.

1.1.3 Interface Description and Administrative Status

You can configure a name for an interface to identify the interface and help you remember the functions of the interface.

You can enter the interface configuration mode to enable or disable an interface.

1. Interface Description

You can configure the name of an interface based on the purpose of the interface. For example, if you want to assign GigabitEthernet 1/1 for exclusive use by user A, you can describe the interface as "Port for User A."

2. Interface Administrative Status

In some cases, you may need to disable an interface. You can directly disable an interface by setting c. If an interface is disabled, it does not receive or send any frames, and the interface loses all its corresponding functions. You can also enable a disabled interface again by setting the management status. Two administrative statuses are available for an interface: **Up** and **Down**. The administrative status of an interface is **Down** when the interface is disabled, and **Up** when the interface is enabled.

1.1.4 MTU of an Interface

You can configure the maximum transmission unit (MTU) of an interface to limit the length of a frame that can be received or forwarded through this interface.

You can set the system MTU to control the maximum length of frames that can be received or forwarded through all interfaces.

When a large amount of data is exchanged over an interface, a frame may be greater than a standard Ethernet frame in length. This type of frame is called jumbo frame. The MTU is the length of the valid data segment in a frame. It does not include the Ethernet encapsulation overhead.

If an interface receives or forwards a frame with a length greater than the MTU, this frame will be discarded.

1.1.5 Configuring Bandwidth of an Interface

The **bandwidth** command can be configured so that some routing protocols (for example, OSPF) can calculate the route metric and the Resource Reservation Protocol (RSVP) can calculate the reserved bandwidth. Modifying the interface bandwidth will not affect the data transmission rate of the physical port.

The **bandwidth** command is a routing parameter, and does not affect the bandwidth of a physical link.

1.1.6 Configuring Carrier Delay

The carrier delay refers to the delay after which the data carrier detect (DCD) signal changes from **Down** to **Up** or from **Up** to **Down**. If the DCD status changes during the delay, the system will ignore this change to avoid negotiation at the upper data link layer. If this parameter is set to a great value, nearly every DCD change is not detected. On the contrary, if the parameter is set to 0, every DCD signal change will be detected, resulting in poor stability.

If the DCD carrier is interrupted for a long time, the carrier delay should be set longer to accelerate convergence of the topology or route. On the contrary, if the DCD carrier interruption time is shorter than the topology or route convergence time, the carrier delay should be set to a greater value to avoid topology or route flapping.

1.1.7 Link Trap Policy

You can enable or disable the link trap function on an interface.

When the link trap function on an interface is enabled, the Simple Network Management Protocol (SNMP) sends link traps when the link status changes on the interface.

1.1.8 Interface Index Persistence

Like the interface name, the interface index also identifies an interface. When an interface is created, the system automatically assigns a unique index to the interface. The index of an interface may change after the device is restarted. You can enable the interface index persistence function so that the interface index remains unchanged after the device is restarted.

After interface index persistence is enabled, the interface index remains unchanged after the device is restarted.

1.1.9 Configuring Routed Port

A physical port on a L3 device can be configured as a routed port, which functions as the gateway interface for L3 switching. The routed port cannot be used for L2 switching. You can run the **no switchport** command to

change a switch port to a routed port and assign an IP address to this port to set up a route. Note that all L2 features of the switch port will be deleted after you run the **no switchport** command.

1.1.10 Configuring L3 AP

Like a L3 routed port, you can run the **no switchport** command to change a L2 AP into a L3 AP on a L3 device, and then assign an IP address to this AP to set up a route. Note that you must delete all L2 features of an AP switch port before running the **no switchport** command.

A L2 AP with one or more member ports cannot be configured as a L3 AP. Similarly, a L3 AP with one or more member ports cannot be changed to a L2 AP.

1.1.11 Configuring Basic Attributes of Interfaces

You can configure the interface rate, duplex mode, flow control mode, and auto negotiation mode of an Ethernet physical port or AP.

1. Interface Rate

Generally, the rate of an Ethernet physical port is determined through auto negotiation with the peer device. The negotiated rate can be any rate within the interface capability. You can also configure any rate within the interface capability for the Ethernet physical port.

When you configure the rate of an AP, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

2. Duplex Mode

The duplex mode of an Ethernet physical port or AP can be configured as follows:

- Full duplex: the interface can receive packets while sending packets.
- Half duplex: the interface can receive or send packets at a time.
- Auto negotiation: the duplex mode of the interface is determined through auto negotiation between the local interface and peer interface.

When you configure the duplex mode of an AP, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

3. Flow Control

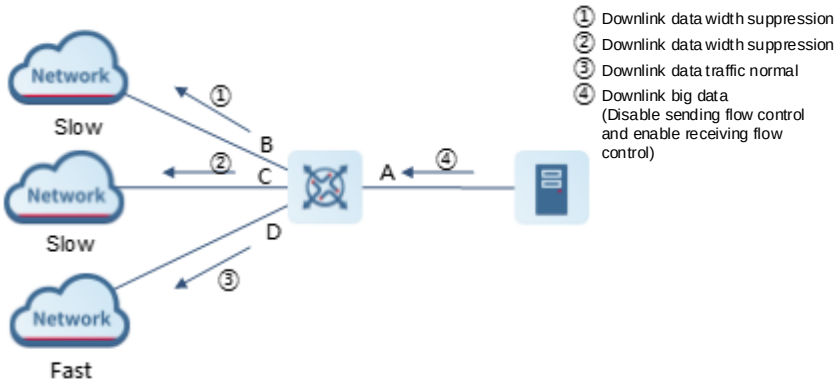
Two flow control modes are defined for an interface:

- Symmetric flow control mode: Generally, after flow control is enabled on an interface, the interface processes the received flow control frames, and sends the flow control frames when congestion occurs on the interface. The received and sent flow control frames are processed in the same way. This is called symmetric flow control mode.
- Asymmetric flow control mode: In some cases, an interface on a device is expected to process the received flow control frames to ensure that no packet is discarded due to congestion, and not to send the flow control frames to avoid decreasing the network speed. In this case, you need to configure the asymmetric flow control mode to separate the procedure for receiving flow control frames from the procedure for sending flow control frames.
- When you configure the flow control mode of an AP, the configuration takes effect on all of its member

ports. (All these member ports are Ethernet physical ports.)

As shown in Figure 1-2, Port A of the device is an uplink port, and Ports B, C and D are downlink ports. Assume that Port A is enabled with the functions of sending and receiving flow control frames. Port B and Port C are connected to different slow networks. If a large amount of data is sent on Port B and Port C, Port B and Port C will be congested, and consequently congestion occurs in the inbound direction of Port A. Therefore, Port A sends flow control frames. When the uplink device responds to the flow control frames, it reduces the data flow sent to Port A, which indirectly slows down the network speed on Port D. In this case, you can disable the function of sending flow control frames on Port A to ensure the bandwidth usage of the entire network.

Figure 1-2 Interface Flow Control Diagram



4. Auto Negotiation Mode

- The auto negotiation mode of an interface can be On or Off. The auto negotiation state of an interface is not completely equivalent to the auto negotiation mode. The auto negotiation state of an interface is jointly determined by the interface rate, duplex mode, flow control mode, and auto negotiation mode.
- When you configure the auto negotiation mode of an AP, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

Note

- Generally, if one of the interface rate, duplex mode, and flow control mode is set to **Auto**, or the auto negotiation mode of an interface is **On**, the auto negotiation state of the interface is **On**, that is, the auto negotiation function of the interface is enabled. If none of the interface rate, duplex mode, and flow control mode is set to **Auto**, and the auto negotiation mode of an interface is **Off**, the auto negotiation function of the interface is disabled.
- For a 100M fiber port, the auto negotiation function is always disabled. For a Gigabit copper port, the auto negotiation function is always enabled, that is, the auto negotiation state is **On**.

1.1.12 Automatic Module Detection

If the interface rate is set to auto, the interface rate can be automatically adjusted based on the type of the inserted module.

Currently, the automatic module detection function can be used to detect only small form-factor pluggable (SFP) and enhanced SFP (SFP+) modules. The SFP module is a Gigabit module, whereas the SFP+ module is a 10

Gigabit module. If an SFP module is inserted, the interface works in Gigabit mode. If an SFP+ module is inserted, the interface works in 10 Gigabit mode.

Note

The automatic module detection function takes effect only when the interface rate is set to auto.

1.1.13 Protected Port

In some application environments, it is required that communication be disabled between some ports on the device. For this purpose, you can configure some ports as protected ports. You can also disable routing between protected ports. After ports are configured as protected ports, the protected ports cannot communicate with each other, but can communicate with non-protected ports. Protected ports work in either of the two modes.

- In the first mode, L2 switching is blocked but routing is allowed between protected ports, which is the default mode.
- In the second mode, L2 switching and routing are both blocked between protected ports.

When two protected ports are configured as a pair of mirroring ports, frames sent or received by the source port can be mirrored to the destination port. Currently, only an Ethernet physical port or AP can be configured as a protected port. When an AP is configured as a protected port, all of its member ports are configured as protected ports. By default, the L3 routing between protected ports is not blocked. In this case, you can run the **protected-ports route-deny** command to block the routing between protected ports.

1.1.14 Port Errdisable Recovery

Some protocols support the port errdisable recovery function to ensure security and stability of the network. For example, in the port security protocol, when you enable port security and configure the maximum number of security addresses on the port, a port violation event is generated if the number of addresses learned on this port exceeds the maximum number of security addresses. Protocols, such as the Spanning Tree Protocol (STP), DOT1X, and REUP, support the similar functions, and a violating port will be automatically shut down to ensure security. Also, if frequent port flapping occurs, a violating port will be shut down.

When a port is disabled because it is set to the errdisable state by the REUP link state tracking group function, the port can be restored only by REUP at a scheduled time or by running the REUP errdisable recovery command in the global configuration mode. In other scenarios, you can run the errdisable recovery command in the global configuration mode to recover all the ports in errdisable state and enable these ports. You can manually recover a port, or automatically recover a port at a scheduled time. You can run the **shutdown** or **no shutdown** command to recover all the ports in the errdisable state and enable these ports.

1.1.15 Optical Module Alarm Detection

After this function is configured, you can view the optical module alarm information of an interface by using the management information base (MIB). When events such as insertion or removal of an optical module, optical module exceptions, and optical module exception clearing are detected, related TRAP messages are sent. The exceptions include overhigh/overlow transmit power of the optical module, overhigh/overlow receive power of the optical module, inter-integrated circuit (IIC) fault of the optical module, unsupported module type, and the like.

After the alarm detection function is enabled and a corresponding detection period is configured, the SNMP device periodically monitors the optical module status on an interface. When any of the above events is detected, the SNMP device sends a related TRAP message. The SNMP device sends a TRAP message immediately for the optical module insertion or removal, but sends a TRAP message in the next period for optical module exceptions and optical module exception clearing. Only one TRAP message is sent for the same exceptions. The exception will be notified periodically, and the exception clearing event will be notified once only. You can disable the periodic notification function by using the repeated notification mode switch.

1.1.16 Optical Module Antifake Detection

You can configure the optical module antifake detection function to check whether the optical module in use is supplied by Ruijie Networks.

If the optical module is not supplied by Ruijie Networks, the data communication may be affected. If the optical module antifake detection function is enabled, the device can automatically identify an optical module that is not supplied by Ruijie Networks and generate an alarm when such module is inserted to the Ruijie device.

This function is disabled by default. You can enable this function through configuration.

Each optical module supplied by Ruijie Networks has a unique antifake code. The device can read this antifake code to determine whether the module is supplied by Ruijie Networks. If not, the device will generate syslogs and send trap messages.

1.1.17 Splitting and Combination of 40G/100G Interfaces

The 40G/100G Ethernet interface is a high-bandwidth interface. It is mainly used on devices at the convergence layer or core layer to increase the interface bandwidth. 40G/100G interface splitting means splitting one 40G/100G interface into four 10G/25G interfaces. In this case, the 40G/100G interface becomes unavailable, and the four 10G/25G interfaces forward data independently. 40G/100G interface combination means combining four 10G/25G interfaces into one 40G/100G interface. In this case, the four 10G/25G interfaces become unavailable, and only the 40G/100G interface forwards data. Unavailable interfaces cannot forward data. You can flexibly adjust the bandwidth by combining or splitting interfaces.

1.1.18 Configuring Interface Traffic Statistics

By default, virtual interfaces such as sub-interfaces and SVIs do not support interface traffic statistics collection, while the Ethernet port and Ethernet AP support interface traffic statistics collection, but do not support IP traffic statistics collection. When you need to locate a network fault or monitor the network operation status, you can enable the interface traffic statistics collection function and IP traffic statistics collection function. And run he **show interface** *interface-type interface-number* command to view the packet statistics of the specified interface and IP packet statistics.

Note

Enabling the interface traffic statistics collection function and IP traffic statistics collection function consumes system resources. You are advised to configure the functions as required.

1.1.19 EEE

Energy Efficient Ethernet (EEE) is an Ethernet solution that saves energy When EEE is enabled, the port enters low power consumption mode when the Ethernet connection is idle, thus saving energy.

Low Power Idle (LPI) is the low power consumption mode. After a port enters LPI mode, it reduces signals significantly, and sends only signals that are sufficient to maintain the connection on the port to save energy.

According to the Ethernet standards or specifications, interfaces with a bandwidth of 100M or above have the active idle state. An interface will consume much power if it maintains connection without being affected by data transmission. Therefore, the power consumption is high no matter whether any data is transmitted on the link. Even if no data is transmitted, the port will always send the idle signals to retain the connection state of the link.

EEE enables a port of the device to enter the LPI mode for the purpose of saving energy. In LPI mode, the power consumption is low when the link is idle. The EEE technology can also quickly change the LPI state of a port to the normal state, providing high-performance data transmission.

After enabled with EEE, the port automatically enters LPI mode if the port is always **Up** without sending or receiving any packet in a period of time. The port recovers the working mode when it needs to send or receive packets, thus saving energy. To make the EEE function take effect, the peer port must also support the EEE function.

Note

Only a copper port working in 100M or 1000M rate mode supports the EEE function.

The EEE function takes effect only on the port enabled with auto negotiation.

1.1.20 Port Flapping Protection

When flapping occurs on a port, a lot of hardware interruptions occur, consuming a lot of CPU resources. On the other hand, frequent port flapping damages the port. You can configure the flapping protection function to protect ports.

By default, the port flapping protection function is enabled. You can disable this function as required. When flapping occurs on a port, the port detects flapping every 2s or 10s. If flapping occurs six times within 2s on a port, the device displays a prompt. If 10 prompts are displayed continuously, that is, port flapping is detected continuously within 20s, the port is shut down (the violation cause shows **Link Dither**). If flapping occurs 10 times within 10s on a port, the device displays a prompt without shutting down the port.

1.1.21 Interface Syslog

You can use the syslog function to determine whether to display information about interface changes or exceptions.

You can enable or disable the syslog function as required. By default, this function is enabled. When an interface becomes abnormal, for example, the interface status changes, or the interface receives error frames, or flapping occurs, the system displays prompts to notify users.

1.1.22 Configuring the MAC Address of an Interface

By default, each Ethernet interface has a globally unique Media Access Control (MAC) address. The MAC addresses of Ethernet interfaces can be modified if required. However, MAC addresses in the same LAN must be unique.

To configure the MAC address of an Ethernet interface, run the **mac-address** command in interface configuration mode:

Note

Configuration of MAC addresses may affect internal communication in a LAN. Therefore, you are not advised to configure MAC addresses by yourself unless necessary.

1.1.23 VLAN Encapsulation Flag on Interfaces

Virtual local area network (VLAN) is a logical network divided on a physical network and corresponds to the L2 network in the ISO model. In 1999, IEEE released the 802.1Q protocol draft for standardizing the VLAN implementation solution.

The VLAN technology enables the network administrator to divide one physical LAN into multiple broadcast domains (or VLANs). Each VLAN contains a group of workstations with the same requirements and each VLAN has the same attributes as the physical LAN. As VLANs are logically divided, workstations in the same VLAN do not need to be placed in the same physical space, that is, these workstations may belong to different physical LAN network segments. Multicast and unicast traffic in a VLAN will not be forwarded to other VLANs. This helps control traffic, reduces device investment, simplifies network management, and improves the network security.

VLAN is a protocol used to solve Ethernet broadcast and security problems. During packet transmission, a VLAN header is added to Ethernet frames. In addition, VLAN IDs are used to classify users to different work groups to restrict L2 exchange between users in different work groups. Each work group is a VLAN. VLANs can be used to restrict the broadcast scope and form virtual work groups to manage networks dynamically.

To ensure communication with hosts in a VLAN, you can configure the 802.1Q (VLAN protocol) VLAN encapsulation flag on the Ethernet interface or sub-interface. In this case, when packets are sent over the Ethernet interface, the corresponding VLAN header will be encapsulated. When packets are received, the VLAN header will be deleted from the packet.

1.1.24 Configuring the FEC Mode of an Interface

Forward error correction (FEC) is an error code correction method employing the following working principle: The sender adds a redundancy error-correcting code to the data for sending. The receiver performs error detection on the data based on the error-correcting code. If an error is found, the receiver corrects the error. FEC improves signal quality but also causes signal delay. Users can enable or disable this function according to the actual situation.

There are three FEC modes: rs mode, base-r mode, and auto mode. Different types of interfaces support different FEC modes, depending on the specific products.

1.1.25 Configuring the Sampling Period of Ethernet Interface Statistics

The default statistics sampling period of an Ethernet interface or Ethernet sub-interface is 5 seconds, which means that interface statistics are updated every 5 seconds. In scenarios with high requirements for real-time statistics, you can prolong the sampling period.

A shorter sampling period indicates higher system performance consumption. Therefore, the sampling period must be adjusted as required. If the number of physical ports exceeds 500, you are advised to set the sampling period to a value greater than 10s.

1.1.26 Configuring Enhanced Name Display for Interfaces

After enhanced name display for interfaces is enabled in the standard MIB node, the value of an interface name node in the standard MIB does not contain spaces. In addition, the ifName node displays the full name of the interface, which does not contain spaces. By default, the value and interface name of the interface name node in the standard MIB contain spaces, and the ifName node displays the short name of the interface.

1.1.27 Including Interframe Gaps in Interface Packet Rate Statistics

By default, interframe gaps are not included in the statistics of packet sending/receiving rate of Ruijie device. You can enable the function of including interframe gaps in interface packet rate statistics, if you want to view the statistics at the physical layer, which contains the number of bytes of packets and the interframe gap. The packet sending/receiving rate at the physical layer refers to the sending/receiving rate of packets that contains interframe gaps.

After this function is enabled, the size of the interframe gap is fixed to 20 bytes. (The interframe gap consists of 12 bytes and the preamble consists of 8 bytes.) An error exists because the chip collects statistics on the frame gap of 20 bytes, but the command statistics exclude the frame gap.

1.2 Configuration Task Summary

The Ethernet interface configuration includes the following tasks:

(1) Configuring Basic Features

(2) (Optional) Configuring Interface Attributes

1.3 Configuring Basic Features

1.3.1 Overview

- Create a specified logical interface and enter the configuration mode of this interface, or enter the configuration mode of an existing physical or logical interface.
- Create multiple specified logical interfaces and enter interface configuration mode, or enter configuration mode of multiple existing physical or logical interfaces.
- The interface indexes remain unchanged after the device is restarted.
- Configure the interface description so that users can directly learn information about the interface.
- Enable or disable the link trap function of an interface.
- Configure the interface administrative status, and enable or disable an interface.
- Split a 40G interface or combine four 10G interfaces into one 40G interface.
- Enable enhanced name display for interfaces.

1.3.2 Restrictions and Guidelines

- The **no** form of the command can be used to delete a specified logical interface or logical interfaces in a specified range, but cannot be used to delete a physical port or physical ports in a specified range.
- The **default** form of the command can be used in the interface configuration mode to restore default settings of a specified physical port or a logical interface, or interfaces or ports in a specified range.

- The errdisbale ports can be recovered by using the **shutdown** or **no shutdown** command. To prevent unwanted link flapping caused by frequent operation of the **shutdown/no shutdown** command, there should be a certain time interval (which must be greater than the carrier delay of the interface) before/after configuring the **shutdown**/**no shutdown** command twice on an interface.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure a single interface.

interface *interface-type interface-number*

The physical port has been created by default.

(4) (Optional) Configure interfaces within a range.

interface range { *port-range* | **macro** *macro-name* }

The port range is not specified by default.

(5) (Optional) Configure interface index persistence.

snmp-server if-index persist

The interface index persistence function is disabled by default.

(6) (Optional) Configure splitting and combination of 40G interfaces.

split interface *interface-type interface-number*

The 40G interface is unsplit by default.

(7) (Optional) Configure the port flapping protection function.

physical-port dither protect

The port flapping protection function is enabled by default.

(8) (Optional) Configure the syslog information printing function for the interface.

logging [**link-updown** | **error-frame** | **link-dither** | **res-lack-frame** | **crc-frame**]

The interface information printing function is disabled by default.

(9) Enter the interface configuration mode.

interface *interface-type interface-number*

(10) (Optional) Configure the description of an Interface.

description *interface-name*

No interface name is configured by default.

(11) (Optional) Configure the LinkTrap function of an interface.

snmp trap link-status

The LinkTrap notification sending function for interface status changes is enabled by default.

(12) (Optional) Configure the administrative status of an interface.

shutdown

The interface is in **Up** state by default.

1.4 Configuring Interface Attributes

1.4.1 Overview

- Enable the device to connect and communicate with other devices through the switch port or routed port.
- Adjust various interface attributes on the device.

1.4.2 Restrictions and Guidelines

- You can select either fiber or copper as the medium type of an interface when both medium types are available. Once the medium type is selected, all interface attributes, including the status, duplex mode, and rate, are configured for the interface of the selected medium type. If the interface type is changed, the attributes of the new interface type are the default attributes. You can reconfigure these attributes as required.
- When the FEC function is enabled at one end of the link, it must be also enabled at the other end. If the QSFP28-100G-LR4 optical module is used without affecting the negotiation status of the two ends, the FEC function is disabled by default and should not be enabled according to the IEEE standard protocol. If the QSFP28 optical modules other than QSFP28-100G-LR4 are used, the FEC function is enabled by default, and disabling this function may lead to packet errors.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the system MTU.

system mtu *mtu-value*

Configuring the MTU of the system will update the MTU effective values of all the Ethernet interfaces (including the APs) of the system. However, if the interface is configured with an MTU, the MTU configured for the interface will take effect.

The MTU of the system is not configured by default.

(4) (Optional) Configure the forwarding plane MTU.

mtu forwarding *number*

The command works on all the physical ports only and controls only the forwarding of L2 packets. After the command is configured, the protocol MTU is inconsistent with the chip forwarding MTU, which may cause problems such as flow interruption and protocol exception in some scenarios. For example, in the IPv6 scenario, if the global fwd_mtu configuration is smaller than the default interface value when the default MTU is configured for the interface, the IPv6 packet cannot be sent and received normally, and the network will be interrupted. You are advised to use the **system mtu** command instead of this command unless there are special scenario requirements.

(5) (Optional) Configure optical module antifake detection.

fiber antifake { **ignore** | **enable** }

The optical module antifake detection function is disabled by default.

(6) (Optional) Configure the sampling period of Ethernet interface statistics.

ethernet-port counter sample-period [*interval*]

The sampling period of Ethernet interface statistics is 5s by default.

(7) (Optional) Configure the sampling period of Ethernet sub-interface statistics.

ethernet-subport counter route-sample-period [*interval*]

The sampling period of Ethernet sub-interface statistics is 5s by default.

(8) (Optional) Include interframe gaps in port rate statistics.

flow-statistics include-interframe enable

The packet sending and receiving rate statistics are cleared and recalculated after you run this command.

The function of including interframe gaps in interface packet rate statistics is disabled by default.

(9) Enter the interface configuration mode.

interface *interface-type interface-number*

(10) (Optional) Configure a L3 AP.

no switchport

(11) (Optional) Configure the rate of an interface.

speed [**10** | **100** | **1000** | **10G** | **40G** | **auto**]

If an interface is an AP member port, the rate of this interface is determined by the rate of the AP. When the interface exits the AP, it uses its own rate configuration. You can run the **show interfaces** command to view the rate configuration. The rate options available to an interface vary with the type of the interface. For example, you cannot set the rate of an SFP interface to 10 Mbps.

(12) (Optional) Configure the duplex mode of an interface.

duplex { **auto** | **full** | **half** }

(13) (Optional) Configure the flow control mode of an interface.

flowcontrol { **auto** | **off** | **on** | **receive** { **auto** | **off** | **on** } | **send** { **auto** | **off** | **on** } }

Flow control is disabled by default.

(14) (Optional) Configure the auto negotiation mode of an interface.

negotiation mode { **on** | **off** }

The auto negotiation mode is disabled by default.

(15) (Optional) Configure the MTU of an interface.

mtu *num-value*

By default, the MTU of an interface is usually 1500 bytes. The configuration varies with different interface types. The actual conditions of the specific interface prevail.

(16) (Optional) Configure the bandwidth of an interface.

bandwidth *kilobits*

No interface bandwidth is configured by default.

(17) (Optional) Configure the carrier delay of an interface.

carrier-delay { [**milliseconds**] *delay-interval* | **up** [**milliseconds**] *up-interval* **down** [**milliseconds**] *down-interval* }

The carrier delay of an interface is 2s by default.

(18) (Optional) Configure the load interval of an interface.

load-interval *seconds*

The interval of load calculation for an interface is 10s by default.

(19) (Optional) Configure a protected port.

switchport protected

A protected port is not configured for the port by default.

(20) (Optional) (In global configuration mode) Configure L3 routing blocking between protected ports.

protected-ports route-deny

The L3 routing blocking function between protected ports is disabled by default.

(21) (Optional) Configure port errdisable recovery.

errdisable recovery [**interval** *interval* | **cause** *link-state*]

The port errdisable recovery function is disabled by default.

(22) (Optional) Configure the interface traffic statistics collection function.

statistics { **enable** | **ip enable** }

The IP traffic statistics collection function is disabled for all the interfaces by default.

(23) (Optional) Create an Ethernet sub-interface.

interface gigabitethernet 0/1.1

No Ethernet sub-interface is created by default.

(24) (Optional) Configure the FEC mode of an interface.

fec mode { **rs | base-r** | **none** | **auto** }

By default, the FEC mode of an interface depends on the interface type, and a specific FEC mode is subject to the actual product.

1.5 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

You can run the **clear** commands to clear information.

Caution

Services may be interrupted due to loss of vital information if you run the **clear** command during device operation.

The administrator can run the **line-detect** command to check the operating status of a cable. Line detection helps determine the operating status of a cable when the cable is short-circuited, disconnected, or in another abnormal state.

Specification

Only a physical port using copper as the medium supports line detection. A physical port using fiber as the medium or an AP does not support line detection.

When line detection is performed on an operational interface, the interface will be temporarily disconnected, and then re-connected.

Table 1-1 Ethernet Interface Monitoring

Command	Purpose
show interfaces [*interface-type interface-number*]	Displays all the statuses and configuration information of a specified interface.
show interfaces [*interface-type interface-number*] **status err-disabled**	Displays the interface errdisable status.
show interfaces [*interface-type interface-number*] **link-state-change statistics**	Displays the link status change time and count of a specified port.
show interfaces [*interface-type interface-number*] **switchport**	Displays the administrative and operational states of switch interfaces (non-routed interfaces).
show interfaces [*interface-type interface-number*] **description** [**up | down**]	Displays the description and status of a specified interface.
show interfaces [*interface-type interface-number*] **counters** [**up | down**]	Displays the statistics of a specified port, among which the displayed rate may contain an error of ±0.5%.
show interfaces [*interface-type interface-number*] **counters increment** [**up** | **down**]	Displays the number of packets added in the previous sampling interval.
show interfaces [*interface-type interface-number*] **counters error** [**up** | **down**] [**nozero**]	Displays the statistics about error packets.
show interfaces [*interface-type interface-number*] **counters rate** [**up | down**] [**nozero**]	Displays the packet sending/receiving rate of the interface.

Command	Purpose
show interfaces [*interface-type interface-number*] **counters rate physical-layer** [**up** | **down**] [**nozero**]	Displays the packet sending/receiving rate of an interface at the physical layer. The packet sending/receiving rate at the physical layer refers to the sending/receiving rate of packets that contains interframe gaps.
show interfaces [*interface-type interface-number*] **counters summary** [**up** | **down**] [**nozero**]	Displays a summary of interface packets.
show interfaces [*interface-type interface-number*] **counters drops** [**up | down**]	Displays the statistics of discarded packets of an interface.
show interfaces [*interface-type interface-number*] **line-detect**	Displays the line detection status. Line detection helps determine the operating status of a cable when the cable is short-circuited, disconnected, or in another abnormal state.
show interfaces [*interface-type interface-number*] **usage** [**up | down**]	Displays the bandwidth usage of an interface.
show interface [*interface-type interface-number*] **mtu forwarding**	Displays the information of the forwarding plane MTU.
show mgmt virtual	Displays the information of the virtual management port.
show vlans	Displays the information of a VLAN sub-interface.
show interfaces [*interface-type interface-number*] **transceiver**	Displays the basic information about the optical module on a specified interface.
show interfaces [*interface-type interface-number*] **transceiver alarm**	Displays the current fault alarms of the optical module on a specified interface. If no fault occurs, **None** is displayed.
show interfaces [*interface-type interface-number*] **transceiver diagnosis**	Displays the current measurement values of optical module diagnosis parameters of a specified interface.
show split summary	Displays the splitting and combination information of 40G/100G interfaces.
clear counters [*interface-type interface-number*]	Clears the statistics of a specified interface.
clear link-state-change statistics [*interface-type interface-number*]	Clears the statistics of link status changes of an interface.

Command	Purpose
show interfaces [*interface-type interface-number*] **troubleshooting**	Displays the diagnosis information of an interface.
show interfaces [*interface-type interface-number*] **fault-info**	Displays the fault information of an interface, including the fault cause and occurrence time.

1.6 Configuration Examples

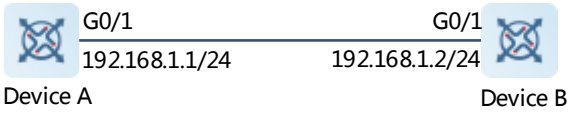
1.6.1 Configuring Interface Attributes

1. Requirements

Interconnect two devices, and configure the basic attributes of the device interfaces.

2. Topology

Figure 1-3 Interface Attribute Topology



3. Notes

- Connect two devices through the switch ports.
- Configure an SVI on each of the two devices, and assign IP addresses in the same network segment to the two SVIs.
- Enable interface index persistence on the two devices.
- Enable the link trap function on the two devices.
- Configure the interface administrative status on the two devices.

4. Procedure

Configure as follows on Device A.

```
DeviceA> enable
DeviceA # configure terminal
DeviceA(config)# snmp-server if-index persist
DeviceA(config)# interface vlan 1
DeviceA(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0
DeviceA(config-if-VLAN 1)# exit
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# snmp trap link-status
DeviceA(config-if-GigabitEthernet 0/1)# shutdown
```

Configure as follows on Device B.

```
DeviceB# configure terminal
DeviceB(config)# snmp-server if-index persist
DeviceB(config)# interface vlan 1
DeviceB(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0
DeviceB(config-if-VLAN 1)# exit
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# snmp trap link-status
DeviceB(config-if-GigabitEthernet 0/1)# shutdown
```

5. Verification

Perform verification on Device A and Device B as follows:

- Run the **shutdown** command on the interface GigabitEthern 0/1, and check whether GigabitEthern 0/1 and SVI 1 are in **Down** state.
- Run the **shutdown** command on the interface GigabitEthern 0/1, and check whether a trap message indicating the **Down** state of this interface is sent.
- Restart the device, and check whether the interface index of GigabitEthern 0/1 is the same as that before the restart.

Device A:

```
DeviceB # show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is administratively down  , line protocol is DOWN
Hardware is GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Queue    Transmitted packets    Transmitted bytes      Dropped packets
Dropped bytes
     0                 0                 0                 0                 0
     1                 0                 0                 0                 0
     2                 0                 0                 0                 0
     3                 0                 0                 0                 0
     4                 0                 0                 0                 0
     5                 0                 0                 0                 0
     6                 0                 0                 0                 0
     7                 4               440                 0                 0
  Switchport attributes:
    interface's description:""
    lastchange time:0 Day:20 Hour:15 Minute:22 Second
    Priority is 0
    admin medium-type is Copper, oper medium-type is Copper   admin duplex mode is
AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
```

```
    flow control admin status is OFF, flow control oper status is Unknown
    admin negotiation mode is OFF, oper negotiation state is ON
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Port-type: access
    Vlan id: 1
   10 seconds input rate 0 bits/sec, 0 packets/sec
   10 seconds output rate 0 bits/sec, 0 packets/sec
    4 packets input, 408 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    4 packets output, 408 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
A# show interfaces vlan 1
Index(dec):4097 (hex):1001
VLAN 1 is UP  , line protocol is DOWN
Hardware is  VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af)
Interface address is: 192.168.1.1/24
ARP type: ARPA, ARP Timeout: 3600 seconds
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 0/255, Txload is 0/255
```

Device B:

```
DeviceB# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is administratively down  , line protocol is DOWN
Hardware is GigabitEthernet
Interface address is: no ip address, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Queue    Transmitted packets    Transmitted bytes      Dropped packets
Dropped bytes
     0                  0                  0                  0                  0
     1                  0                  0                  0                  0
     2                  0                  0                  0                  0
     3                  0                  0                  0                  0
     4                  0                  0                  0                  0
     5                  0                  0                  0                  0
     6                  0                  0                  0                  0
     7                  4                440                  0                  0
  Switchport attributes:
    interface's description:""
```

```
    lastchange time:0 Day:20 Hour:15 Minute:22 Second
    Priority is 0
    admin medium-type is Copper, oper medium-type is Copper
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow control admin status is OFF, flow control oper status is Unknown
    admin negotiation mode is OFF, oper negotiation state is ON
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Port-type: access
    Vlan id: 1
   10 seconds input rate 0 bits/sec, 0 packets/sec
   10 seconds output rate 0 bits/sec, 0 packets/sec
    4 packets input, 408 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    4 packets output, 408 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
B# show interfaces vlan 1
Index(dec):4097 (hex):1001
VLAN 1 is UP  , line protocol is DOWN
Hardware is  VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af)
Interface address is: 192.168.1.2/24
ARP type: ARPA, ARP Timeout: 3600 seconds
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 0/255, Txload is 0/255
```

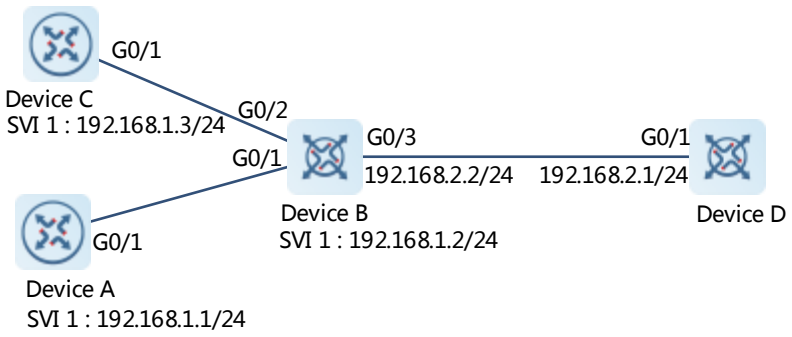
1.6.2 Configuring Interconnection Interfaces

1. Requirements

Interconnect two devices, and configure attributes of the device interfaces.

2. Topology

Figure 1-4 Interconnection Interface Configuration Topology



3. Notes

- On Device A, configure GigabitEthernet 0/1 as a switch port in access mode, with the default VLAN ID as 1. Configure SVI 1, assign an IP address to SVI 1, and set up a route to Switch D.
- On Device B, configure GigabitEthernet 0/1 and GigabitEthernet 0/2 as switch ports in trunk mode, with the native VLAN ID as 1. Configure SVI 1, and assign an IP address to SVI 1. Configure GigabitEthernet 0/3 as a routed port, and assign an IP address in another network segment to this port.
- On Device C, configure GigabitEthernet 0/1 as a switch port in access mode, with the default VLAN ID as 1. Configure SVI 1, and assign an IP address to SVI 1.
- On Device D, configure GigabitEthernet 0/1 as a routed port, assign an IP address to this port, and set up a route to Switch A.

4. Procedure

Configure as follows on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode access
DeviceA(config-if-GigabitEthernet 0/1)# switchport access vlan 1
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface vlan 1
DeviceA(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0
DeviceA(config-if-VLAN 1)# exit
DeviceA(config)# ip route 192.168.2.0 255.255.255.0 VLAN 1 192.168.1.2
```

Configure as follows on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface GigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/1)# exit
DeviceB(config)# interface GigabitEthernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/2)# exit
DeviceB(config)# interface vlan 1
DeviceB(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0
DeviceB(config-if-VLAN 1)# exit
DeviceB(config)# interface GigabitEthernet 0/3
DeviceB(config-if-GigabitEthernet 0/3)# no switchport
DeviceB(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/3)# exit
```

Configure as follows on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# interface GigabitEthernet 0/1
```

```
DeviceC(config-if-GigabitEthernet 0/1)# port-group 1
DeviceC(config-if-GigabitEthernet 0/1)# exit
DeviceC(config)# interface aggregateport 1
DeviceC(config-if-AggregatePort 1)# switchport mode access
DeviceC(config-if-AggregatePort 1)# switchport access vlan 1
DeviceC(config-if-AggregatePort 1)# exit
DeviceC(config)# interface vlan 1
DeviceC(config-if-VLAN 1)# ip address 192.168.1.3 255.255.255.0
DeviceC(config-if-VLAN 1)# exit
```

Configure as follows on Device D.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# interface GigabitEthernet 0/1
DeviceD(config-if-GigabitEthernet 0/1)# no switchport
DeviceD(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
DeviceD(config-if-GigabitEthernet 0/1)# exit
DeviceD(config)# ip route 192.168.1.0 255.255.255.0  GigabitEthernet 0/1 192.168.2.2
```

5. Verification

Perform verification on Device A, Device B, Device C, and Device D as follows:

- On Switch A, ping the IP addresses of interfaces of the other three devices. Verify that you can access the other two on each device.
- Verify that Device B and Device D can be pinged mutually.
- Verify that the interface status is correct. Check the PIM-DM routing tables of Device A and Device B and confirm whether the multicast packets can be received. Device A is taken as an example below:

Check on Device A.

```
DeviceA# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP  , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de90 (bia 00d0.f865.de90)
Interface address is: no ip address
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
    Priority is 0
    Admin medium-type is Copper, oper medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Full
    Admin speed is AUTO, oper speed is 100M
    Flow control admin status is OFF, flow control oper status is OFF
    Admin negotiation mode is OFF, oper negotiation state is ON
```

```
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
Port-type: access
Vlan id: 1
  Rxload is 1/255, Txload is 1/255
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
    362 packets input, 87760 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    363 packets output, 82260 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

Check on Device B.

```
DeviceB# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP  , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de91 (bia 00d0.f865.de91)
Interface address is: no ip address
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
    Priority is 0
    Admin medium-type is Copper, oper medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Full
    Admin speed is AUTO, oper speed is 100M
    Flow control admin status is OFF, flow control oper status is OFF
    Admin negotiation mode is OFF, oper negotiation state is ON
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: trunk
    Native vlan: 1
    Allowed vlan lists: 1-4094
Active vlan lists: 1
  Rxload is 1/255, Txload is 1/255
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
362 packets input, 87760 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
363 packets output, 82260 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

Check on Device C.

```
DeviceC# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP  , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de92 (bia 00d0.f865.de92)
Interface address is: no ip address
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
Last link state change time: 2012-12-22 14:00:48
Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
Priority is 0
Admin medium-type is Copper, oper medium-type is Copper
Admin duplex mode is AUTO, oper duplex is Full
Admin speed is AUTO, oper speed is 100M
Flow control admin status is OFF, flow control oper status is OFF
Admin negotiation mode is OFF, oper negotiation state is ON
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Rxload is 1/255, Txload is 1/255
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
362 packets input, 87760 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
363 packets output, 82260 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

Check on Device D.

```
DeviceD# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP  , line protocol is UP
Hardware is GigabitEthernet, address is 00d0.f865.de93 (bia 00d0.f865.de93)
Interface address is: 192.168.2.1/24
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
Last link state change time: 2012-12-22 14:00:48
Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
Priority is 0
Admin medium-type is Copper, oper medium-type is Copper
Admin duplex mode is AUTO, oper duplex is Full
Admin speed is AUTO, oper speed is 100M
Flow control admin status is OFF, flow control oper status is OFF
Admin negotiation mode is OFF, oper negotiation state is ON
```

```
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Rxload is 1/255, Txload is 1/255
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
362 packets input, 87760 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
363 packets output, 82260 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

Contents

1 Configuring Aggregate Port....1
1.1 Introduction....1
1.1.1 Basic Concepts....1
1.1.2 Load Balancing....5
1.1.3 Member Port BFD Detection....7
1.1.4 Protocols and Standards....7
1.2 Configuration Task Summary....7
1.3 Configuring Static APs....8
1.3.1 Overview....8
1.3.2 Restrictions and Guidelines....8
1.3.3 Procedure....9
1.4 Configuring LACP APs....10
1.4.1 Overview....10
1.4.2 Restrictions and Guidelines....10
1.4.3 Procedure....10
1.5 Enabling LinkTrap....11
1.5.1 Overview....11
1.5.2 Procedure....11
1.6 Configuring a Load Balancing Mode....12
1.6.1 Overview....12
1.6.2 Restrictions and Guidelines....12
1.6.3 Procedure....12

1.7 Configuring an AP Capacity Mode 14
1.7.1 Overview 14
1.7.2 Restrictions and Guidelines 14
1.7.3 Procedure 14
1.8 Enabling BFD for AP Member Ports 14
1.8.1 Overview 14
1.8.2 Restrictions and Guidelines 14
1.8.3 Procedure 15
1.9 Configuring a Preferred AP Member Port 15
1.9.1 Overview 15
1.9.2 Restrictions and Guidelines 15
1.9.3 Procedure 15
1.10 Configuring the Minimum Number of AP Member Ports 16
1.10.1 Overview 16
1.10.2 Restrictions and Guidelines 16
1.10.3 Procedure 16
1.11 Enabling the LACP Independent Port Function 17
1.11.1 Overview 17
1.11.2 Restrictions and Guidelines 17
1.11.3 Procedure 17
1.12 Monitoring 18
1.13 Configuration Examples 19
1.13.1 Configuring Static APs 19
1.13.2 Configuring LACP APs 20

1.13.3 Enabling LinkTrap 22

1.13.4 Configuring a Load Balancing Mode 24

1.13.5 Configuring Hash Load Balancing Control 26

1.13.6 Configuring an AP Capacity Mode 28

1.13.7 Enabling BFD for Member Ports 29

1.13.8 Configuring Interworking Between the Access Device and a Server with Two NICs over a Preferred LACP AP 32

1.13.9 Configuring Automatic Server Deployment over a Preferred LACP AP 34

1.13.10 Configuring the Minimum Number of AP Member Ports (When the Number of AP Member Ports Is Less Than the Minimum Number) 36

1.13.11 Configuring the Minimum Number of AP Member Ports (When the Number of AP Member Ports Is Not Less Than the Minimum Number) 38

1.13.12 Enabling the LACP Independent Port Function 40

1 Configuring Aggregate Port

1.1 Introduction

An aggregate port (AP) is used to bundle multiple physical links into one logical link to increase the link bandwidth and improve connection reliability.

1.1.1 Basic Concepts

An AP supports load balancing, that is, distributes load evenly among member links. Besides, an AP realizes link backup. When a member link of the AP is disconnected, the load carried by the link is automatically allocated to other functional member links. A member link does not forward broadcast or multicast packets to other member links.

- If the link between two devices supports a maximum bandwidth of 1,000 Mbps (assuming that the devices each have a 1,000 Mbps port), when the service traffic carried by the link exceeds 1,000 Mbps, the traffic in excess will be discarded. Port aggregation can be used to solve the problem. For example, you can connect the two devices with network cables and combine multiple links to form a logical link capable of multiples of 1,000 Mbps.
- If the two devices are connected by one network cable, when the link between the two ports of the devices is disconnected, the services carried by the link will be interrupted. After the connected ports are aggregated, the services will not be affected as long as one link remains connected.

There are two kinds of AP link aggregation. One is the static AP mode, and the other is dynamic aggregation through Link Aggregation Control Protocol (LACP).

1. Static AP

The static AP mode means manually configuring physical ports and adding them to an AP aggregation group. An AP in static AP mode is called a static AP, and its member ports are called static AP member ports. The static AP configuration is simple. You only need to run a command to add the specified physical port to the AP. After joining the aggregation group, a member port can receive and transmit data and participate in load balancing within the group.

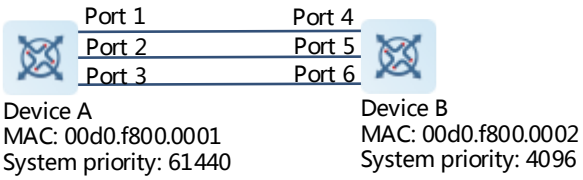
2. Dynamic AP (LACP)

LACP is a protocol about dynamic link aggregation. It exchanges information with the connected device through link aggregation control protocol data units (LACPDU). An AP in LACP mode is called a dynamic AP, and its member ports are called dynamic AP member ports.

An LACP-enabled port sends LACPDUs to advertise its system priority, system MAC address, port priority, port number, and operation key. When receiving the LACPDU from the peer end, the device compares the system priorities of both ends based on the system ID in the packet. The end with a higher system ID priority sets the ports in the aggregation group to **Bundle** state based on the port ID priorities in a descending order, and sends an updated LACPDU. When receiving the LACPDU, the peer end sets corresponding ports to **Bundle** state so that both ends maintain consistency when a port exits or joins the aggregation group. The physical link can forward packets only after the ports at both ends are bundled dynamically.

After link aggregation, the LACP AP member ports periodically exchange LACPDUs. When a port does not receive an LACPDU in the specified time, a timeout occurs and the links are unbundled. In this case, the member ports cannot forward packets. There are two timeout modes: long timeout and short timeout. In long timeout mode, a port sends a packet every 30s. If it does not receive a packet from the peer end in 90s, a timeout occurs. In short timeout mode, a port sends a packet every 1s. If it does not receive a packet from the peer end in 3s, a timeout occurs.

Figure 1-1 LACP Negotiation



As shown in Figure 1-1, Device A is connected to Device B through three ports. Set the system priority of Device A to 61440 and that of Device B to 4096. Enables LACP link aggregation on the three directly connected ports of Device A and Device B, set the aggregation mode of the three ports to the active mode, and set the port priority to the default value 32768.

When receiving an LACPDU from Device A, Device B finds that it has a higher system ID priority than Device A (a smaller value indicates a higher priority). Therefore, Device B sets Port 4, Port 5, and Port 6 to **Bundle** state based on the order of port ID priorities (or in an ascending order of port numbers if the port priorities are the same). When receiving an updated LACPDU from Device B, Device A finds that Device B has a higher system ID priority and has set Port 4, Port 5, and Port 6 to **Bundle** state. Then Device A also sets Port 1, Port 2, and Port 3 to **Bundle** state.

3. AP Member Port Mode

There are three aggregation modes available, namely, active, passive, and static.

AP member ports in active mode initiate LACP negotiation. AP member ports in passive mode only respond to received LACPDUs. AP member ports in static mode do not send LACPDUs for negotiation. The following table lists the requirements for peer port mode.

Table 1-1 Requirements for Peer Port Aggregation in Aggregation Mode

Port Mode	Peer Port Mode
Active mode	Active or passive mode
Passive mode	Active mode
Static Mode	Static Mode

4. AP Member Port State

Static AP member ports can be in **Up** or **Down** state.

- When a member port is **Down**, the port cannot forward packets. The **Down** state is displayed.

- When a member port is **Up** and the link protocol is ready, the port can forward packets. The **Up** state is displayed.

LACP AP member ports has the following three states:

- When the link of a port is **Down**, the port cannot forward packets. The **Down** state is displayed.
- When the link of a port is **Up** and the port is added to an aggregation group (as a member of the aggregation group, the port participates in data packet forwarding of the aggregation group) after LACP negotiation, the **bndl** state is displayed.
- When the link of a port is **Up** but the port is suspended because the peer end is not enabled with LACP or the attributes of the ports are inconsistent with those of the master port, the **susp** state is displayed. (The port in **susp** state does not forward packets.)

Note

- Only full-duplex ports are capable of LACP aggregation.
- LACP aggregation can be implemented only when the rates, flow control approaches, medium types, and L2/L3 attributes of member ports are consistent.
- If you modify the preceding attributes of a member port in the aggregation group, LACP aggregation will fail.
- The ports which are prohibited from joining or exiting an AP cannot be added to or removed from a static AP or an LACP AP.

5. AP Capacity Mode

The maximum number of member ports is fixed, which is equal to the maximum number of APs multiplied by the maximum number of member ports supported by a single AP. If you want to increase the maximum number of APs, the maximum number of member ports supported by a single AP must be reduced, and vice versa. This concerns the AP capacity mode concept. Some devices support the configuration of the AP capacity mode. For example, if the system supports 16,384 member ports, you can select 1024 x 16, 512 x 32, and other AP capacity modes (Maximum number of APs multiplied by the maximum number of member ports supported by a single AP).

6. LACP System ID

By default, all the LACP ports on a device belong to the same LACP aggregation system.

The system is identified by a system ID and each system has a priority, which is a configurable value. The system ID consists of the LACP system priority and MAC address of the device. A lower system priority indicates a higher priority of the system ID. If the system priorities are the same, a smaller MAC address of the device indicates a higher priority of the system ID. The system with an ID of a higher priority determines the port state. The port state of a system with an ID of a lower priority keeps consistent with that of a higher priority.

The LACP system ID can be configured when LACP ports of multiple (a maximum of four) independent devices need to negotiate with the LACP port of a specific device (for example, LACP ports of two independent ASWs need to negotiate with the LACP port of the NC). You can set the system IDs of the LACP ports of independent devices to the same MAC address and configure different device IDs to implement normal negotiation.

7. LACP Device ID

The LACP device ID can be configured when LACP ports of multiple independent devices need to negotiate with the LACP port of a specific device. It must be configured together with the system ID.

8. LACP Port ID

Each port has an independent LACP port priority, which is a configurable value. The port ID consists of the LACP port priority and port number. A smaller port priority indicates a higher priority of the port ID. If the port priorities are the same, a smaller port number indicates a higher priority of the port ID.

9. LACP Master Port

When dynamic member ports are **Up**, LACP selects one of those ports to be the master port based on the rates and duplex modes, ID priorities of the ports in the aggregation group, and the bundling state of the member ports in the **Up** state. Only the ports that have the same attributes as the master port are in **Bundle** state and participate in data forwarding. When the attributes of ports are changed, LACP reselects a master port.

10. Preferred AP Member Port

The preferred AP member port feature is used when an AP is connected to a server with two systems. An AP member port is selected as the preferred port that forwards specified packets (packets of the management VLAN) to the server. These packets will not be distributed to other member ports by load balancing. This ensures the communication with the server.

Caution

Configure the port connected to the management network interface card (NIC) of the server as the preferred AP member port.

Some Linux servers have two systems. For example, an HP server has a master system and remote management system. The master system is a Linux system. The remote management system with Integrated Lights-Out (iLO) provides remote management at the hardware-level. iLO can manage the server remotely even when the master system is restarted. The master system has two NICs bundled into an AP for service processing. The management system uses one of the two NICs for remote management. Because services are separated by different VLANs, the VLAN used by the management system is called a management VLAN. The port of a device connected to a server with two NICs is an AP. The packets of the management VLAN must be sent by the member port connected to the NICs of the server to ensure the communication with the remote management system. You can configure a preferred AP member port to send the packets of the management VLAN.

Caution

For a server with two NICs bundled through LACP, if LACP is not running when the master system is restarted, LACP negotiation fails and the AP is **Down**. In this case, the preferred AP member port is downgraded into a static member port and it is bound to the AP for communication with the remote management system of the server. The preferred AP member port will be enabled with LACP again for negotiation after the Linux system is restarted and LACP runs normally.

11. Minimum Number of AP Member Ports

An AP can be configured with a minimum number of AP member ports. When a member port exits the AP aggregation group, causing the number of member ports to be smaller than the minimum number, the other member ports in the group are unbundled, and the AP is **Down**. When the member port rejoins the group, causing the number of member ports to be greater than the minimum number, the member ports in the group are automatically bundled, and the AP is **Up** again.

12. LACP Independent Ports

In normal cases, LACP independent ports are used for interworking between access switches and servers with two NICs. If the operating system (OS) is not pre-installed when a server with two NICs starts, the OS needs to be installed via the remote preboot execution environment (PXE) OS installation device. Before the OS is installed, the server with two NICs cannot perform LACP negotiation with the access device, and only one NIC can work. In this case, the port on the access device must be able to automatically change to a common Ethernet physical port to ensure normal communication between the server and the remote PXE OS installation device. After the OS is installed and both NICs can run the LACP, the port on the access device must be able to enable the LACP again for negotiation.

Caution

- LACP independent ports can work only at layer 2. After an LACP independent port is enabled through configuration, if the LACP independent port does not receive LACP packets, it automatically changes to a common Ethernet port, which automatically copies the rate, duplex mode, flow control, and VLAN configuration from the AP to ensure port forwarding capabilities.
- An LACP independent port automatically changes to a common Ethernet port only if it does not receive LACP packets within the set timeout period. After the port receives LACP packets, it changes to an LACP AP member port again.

1.1.2 Load Balancing

APs segregate packet flows by using load balancing algorithms based on packet features, such as the source and destination MAC addresses, source and destination IP addresses, and L4 source and destination port numbers. The packet flow with the consistent feature is transmitted by one member link, and different packet flows are evenly distributed to member links. For example, in source MAC address-based load balancing, packets are distributed to the member links based on the source MAC addresses of the packets. Packets with different source MAC addresses are evenly distributed to member links. Packets with the identical source MAC address are forwarded by one member link.

Currently, there are several AP load balancing modes as follows:

- Source MAC address or destination MAC address
- Source MAC address + destination MAC address
- Source IP address or destination IP address
- Source IP address + destination IP address
- Source IP address + destination IP address + L4 source port number + L4 destination port number

Note

- Load balancing based on IP addresses or port numbers is applicable only to L3 packets. When a device enabled with this load balancing method receives L2 packets, it automatically switches to the default load balancing method.
- All the load balancing methods use a load algorithm (hash algorithm) to calculate the member links based on the input parameters of the methods. The input parameters include the source MAC address, destination MAC address, source MAC address + destination MAC address, source IP address, destination IP address, source IP address + destination IP addresses, source IP address + destination IP address + L4 port number and so on. The algorithm ensures that packets with different input parameters are evenly distributed to member links. It does not indicate that these packets are always distributed to different member links. For example, in IP address-based load balancing, two packets with different source and destination IP addresses may be distributed to the same member link through calculation.

1. Enhanced Load Balancing

Enhanced load balancing allows the combination of multiple fields in different types of packets. These fields include **src-mac**, **dst-mac**, **l2-protocol**, **vlan**, **src-port**, and **dst-port** in L2 packets, **src-ip**, **dst-ip**, **protocol**, **l4-src-port**, **l4-dst-port**, **vlan**, **src-port**, **dst-port**, **l2-etype**, **src-mac**, and **dst-mac** in IPv4 packets, **src-ip**, **dst-ip**, **protocol**, **l4-src-port**, **l4-dst-port**, **vlan**, **src-port**, **dst-port**, **l2-etype**, **src-mac**, and **dst-mac** in IPv6 packets; **top-label**, **2nd-label**, **3rd-label**, **src-ip**, **dst-ip**, **vlan**, **src-port**, **dst-port**, **src-mac**, **dst-mac**, **protocol**, **l4-src-port**, **l4-dst-port**, and **l2-etype** in MPLS packets; **vlan**, **src-port**, **src-mac**, **src-ip**, **protocol**, **l4-src-port**, **l4-dst-port**, **l2-etype**, **ing-nick**, **egr-nick**, **dst-port**, **dst-mac**, and **dst-ip** in TRILL packets, and **vlan**, **src-port**, **src-id**, **rx-id**, **ox-id**, **fabric-id**, **dst-port**, and **dst-id** in FCoE packets.

A device enabled with enhanced load balancing first determines the types of packets to be transmitted and performs load balancing based on the specified fields in the packets. For example, the AP performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.

Note

- All the load balancing methods are applicable to L2 and L3 APs. You need to configure proper load distribution methods based on different network environments to fully utilize network bandwidth.
- Perform enhanced load balancing based on the **src-mac**, **dst-mac**, and **vlan** fields in L2 packets, and the **src-ip** field in IPv4 packets. If the incoming packet is an IPv4 packet with an ever-changing source MAC address, the enhanced balancing algorithm does not take effect, because the device performs load balancing only based on the **src-ip** field in the IPv4 packet after finding that it is an IPv4 packet.
- In enhanced load balancing, the MPLS balancing algorithm takes effect only for MPLS L3 VPN packets, but does not take effect for MPLS L2 VPN packets.

2. Hash Load Balancing Control

Hash load balancing enables users to flexibly control load balancing in different scenarios. Currently, Ruijie adopts the following hash load balancing control functions:

Hash disturbance factor: Traffic over APs is hashed for balancing. For two devices of the same type, the same path is calculated for load balancing for the same stream. When the equal-cost multi-path (ECMP) is deployed, the same stream of the two devices may be balanced to the same destination device, resulting in hash polarization. The hash disturbance factor is used to affect the load balancing algorithm. Different disturbance factors are configured for different devices to ensure that different paths are provided for the same stream.

Hash synchronization: To ensure network security, a firewall cluster is deployed between the internal and external networks for traffic cleaning. This requires that both the uplink and downlink traffic of a session is transmitted to the same device in the firewall cluster for processing. The source and destination IP addresses contained in the uplink and downlink streams of a session are reversed. The uplink and downlink streams will be directed to different firewalls in the firewall cluster based on the traditional hash algorithm. The hash synchronization function ensures that uplink and downlink streams of a session be transmitted over the same path.

Flexible hash: In normal cases, the load balancing cluster interworks with multiple ToRs via the ECMP, and the ToRs are required to balance all packets of a session to the same scheduling server. However, when a server is faulty, all session streams will be ordered and balanced again based on the traditional load balancing mechanism of ToRs. In this case, packets of the same session may be balanced to two servers. The flexible hash function ensures that when one link is faulty, traffic on other links is not affected and only the traffic of the faulty link is balanced to other active links. In this case, traffic of a session is balanced to the same server.

Hash algorithm mode: Apply the most appropriate hash algorithm mode to different traffic models, so that when traffic changes, balance can still be kept. For example, if the source and destination MAC addresses of a stream increase by 1 at the same time, configuring the algorithm based on the source and destination MAC addresses cannot keep stream balance. In this case, a suitable hash algorithm mode needs to be applied.

Hash factor acquisition mode: There are an inner layer and an outer layer in the header in each of GRE packets, and other tunnel packets. It can be specified to obtain the hash factor from the inner layer or outer layer, to achieve a better balancing effect. For example, in some scenarios, tunnel packets share the same outer IP address but have different inner IP addresses. In this case, the inner IP address can be specified as the hash factor to achieve an optimal balancing effect.

Note

The performance of hash algorithm mode may vary with different devices.

1.1.3 Member Port BFD Detection

Bidirectional Forwarding Detection (BFD) is a protocol that delivers fast detection of path failures. According to RFC7130, LACP takes 3s to detect link failures even in short timeout mode. All the packets sent to the faulty link during the 3-second period will be dropped. BFD correlation delivers faster failure detection. You can configure BFD on member ports to detect link failure and switch load to other member links in case of a link failure. BFD is classified into IPv4 detection and IPv6 detection, which detect IPv4 and IPv6 paths respectively. When BFD detects that the path on a member port fails, the packets are not distributed to the member port. After BFD is enabled on an AP, BFD sessions are set up on its member ports in forwarding state independently.

1.1.4 Protocols and Standards

- IEEE 802.3ad

1.2 Configuration Task Summary

The AP configuration includes the following tasks:

(1) Configuring Static APs

(2) (Optional) Configuring LACP APs

(3) (Optional) Enabling LinkTrap

(4) (Optional) Configuring a Load Balancing Mode

(5) (Optional) Configuring an AP Capacity Mode

(6) (Optional) Enabling BFD for AP Member Ports

(7) (Optional) Configuring a Preferred AP Member Port

(8) (Optional) Configuring the Minimum Number of AP Member Ports

(9) (Optional) Enabling the LACP Independent Port Function

1.3 Configuring Static APs

1.3.1 Overview

- Configure multiple physical ports as AP member ports to realize link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.
- When a member link of the AP is disconnected, the load carried by the link is automatically allocated to other functional member links.

1.3.2 Restrictions and Guidelines

- Only physical ports can be added to an AP.
- To prevent a transient loop when a member port exits, you need to set the member port to **shutdown** state before it exits the AP.
- The ports of different medium types or port modes cannot be added to the same AP.
- L2 ports can be added to only a L2 AP, and L3 ports can be added to only a L3 AP. The L2/L3 attributes of an AP that contains member ports cannot be modified.
- After a port is added to an AP, the attributes of the port are replaced by those of the AP.
- After a port is removed from an AP, the attributes of the port before the adding to the AP are restored.
- There is continuous traffic at the AP. If an AP member port changes from **Link Up** to **Link Down**, an error may occur in traffic statistics of the AP.
- When the AP includes a member port that supports **port speed-mode** configuration, the AP does not support speed configuration, and the original speed configuration on the AP is automatically cleared. The configured rate of the AP is switched to that of **port speed-mode** for the member port.
- You can run the **port-group** command to add a physical port to a static AP in the interface configuration mode of the specified Ethernet port. If the AP does not exist, it will be created automatically.
- You can run the **port-group mode** command to add a physical port to an LACP AP in the interface configuration mode of the specified physical port. If the AP does not exist, it will be created automatically.
- The AP feature must be configured on the devices at both ends of a link and the AP mode must be the same (static AP or LACP AP).
- After a member port exits the AP, the default configurations of the member port may be restored. The original configurations of AP members are processed in different ways for different functions. You are advised to check and confirm the port configurations after a member port exits an AP.
- After a member port exits an AP, the port is shut down to avoid loops. After confirming that the topology is

normal, you can run **no shutdown** in interface configuration mode to enable the port again.

- If the VLAN resource is in a critical state (the number of configured VLANs and the number of routed ports reach the VLAN capacity values) when a L3 AP member port exits the AP, the port may be switched to a L2 port.
- The AP created on a L3 device that does not support L2 features is a L3 AP; otherwise the AP is a L2 AP.

Warning

- After a port is added to an AP, the attributes of the port are consistent with those of the AP. Therefore, it is generally not allowed to perform configuration on the AP member ports or apply configurations to a specific AP member port. However, some commands or functions (such as the **shutdown** and **no shutdown** commands) can be configured on the AP member ports. When using the AP member ports, you need to check whether the function that you want to configure can take effect on a specific AP member port, and perform the configuration properly.
- The error detection function is unavailable to static aggregation. Member ports are bound if linked up. Therefore, you needs to ensure topology accuracy and negotiated attribute consistency among the member ports.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an Ethernet AP.

interface aggregateport *ap-number*

Perform this configuration on an AP-enabled device. When an Ethernet port needs the aggregation function, create the corresponding Ethernet AP

No AP is configured by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure static AP member ports.

port-group *ap-number*

Perform this configuration on AP-enabled devices. To use the static aggregation function, configure the corresponding static AP member ports.

By default, the Ethernet physical port does not belong to any static AP or LACP AP.

(6) (Optional) Convert L2 APs to L3 APs.

no switchport

The AP is a L2 port by default.

(7) (Optional) Create an Ethernet AP sub-interface.

interface aggregateport *sub-ap-number*

No Ethernet AP sub-interface is configured by default.

1.4 Configuring LACP APs

1.4.1 Overview

- Connected devices perform auto negotiation through LACP to realize dynamic link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.
- When a member link of the AP is disconnected, the load carried by the link is automatically allocated to other functional member links.
- It takes 90s for LACP to detect a link failure in long timeout mode and 3s in short timeout mode.

1.4.2 Restrictions and Guidelines

- After a port exits an LACP AP, the default configurations of the port may be restored. The original configurations of LACP AP members are processed in different ways for different functions. You are advised to check and confirm the port configurations after a member port exits an LACP AP.
- To prevent a transient loop when a member port exits, you need to set the member port to **shutdown** state before it exits the AP.
- Changing the LACP system priority may cause LACP AP member ports to be disaggregated and aggregated again.
- Changing the priority of an LACP AP member port may cause the other member ports to be disaggregated and aggregated again.
- There is continuous traffic at the AP. If an AP member port changes from **Link Up** to **Link Down**, an error may occur in traffic statistics of the AP.
- When the AP includes a member port that supports **port speed-mode** configuration, the AP does not support speed configuration, and the original speed configuration on the AP is automatically cleared. The configured rate of the AP is switched to that of **port speed-mode** for the member port.
- The LACP AP member port configurations at both ends of a link must be consistent.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure LACP AP member ports.

port-group *key-number* **mode** { **active** | **passive** }

By default, the Ethernet physical port does not belong to any LACP AP.

(5) (Optional) Configure the LACP system ID.

lacp system-id *system-id*

Configure the LACP system ID when LACP ports of multiple (a maximum of four) independent devices need to negotiate with the LACP port of a specific device.

The LACP system ID is the system ID (MAC address) of the device by default.

(6) (Optional) Configure the LACP device ID.

lacp device *number*

Configure the LACP device ID when LACP ports of multiple (a maximum of four) independent devices need to negotiate with the LACP port of a specific device.

The device ID is 0 by default.

(7) (Optional) Configure the LACP system priority.

lacp system-priority *system-priority*

Perform this configuration when you need to adjust the system ID priority. A smaller value indicates a higher system ID priority. The device with a higher system ID priority takes precedence in selecting an AP.

The LACP system priority of a port is 32768 by default.

(8) Configure the priority of an LACP AP member port.

lacp port-priority *port-priority*

Perform this configuration when you need to specify the port ID priority. A smaller value indicates a higher port ID priority. The port with the highest port ID priority will be selected as the master port.

The priority of the LACP AP member port is 32768 by default.

(9) Configure the timeout mode of LACP AP member ports.

lacp short-timeout

When you need to implement real-time link failure detection, configure the short timeout mode. A timeout occurs if a port does not receive a packet within 3 seconds in short timeout mode and 90 seconds in long timeout mode.

The timeout mode of an LACP AP member port is long timeout by default.

1.5 Enabling LinkTrap

1.5.1 Overview

Enable the system with LinkTrap to send LinkTrap messages when aggregation links are changed.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the AP interface configuration mode.

interface Aggregateport *ap-interface-number*

(4) (Optional) Configure the LinkTrap function of an AP.

snmp trap link-status

The LinkTrap notification function of an AP is enabled by default.

(5) (Optional) Configure the LinkTrap function of AP member ports.

aggregateport member linktrap

The LinkTrap notification function of AP member ports is disabled by default.

1.6 Configuring a Load Balancing Mode

1.6.1 Overview

- The system distributes incoming packets among member links by using the specified load balancing algorithm. The packet flow with the consistent feature is transmitted by one member link, whereas different packet flows are evenly distributed to various links. A device enabled with enhanced load balancing first determines the types of packets to be transmitted and performs load balancing based on the specified fields in the packets. For example, the AP performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.
- In enhanced load balancing mode, configure the hash disturbance factor to ensure that same packets from two devices of the same type is balanced to different links.
- In enhanced load balancing mode, enable hash synchronization to ensure that uplink and downlink packets of the same type are transmitted over the same link. For example, in load balancing based on the source and destination IP addresses, enable hash synchronization for IPv4 packets to ensure that the uplink and downlink IPv4 packets are transmitted over the same path.
- Enable flexible hash to balance traffic of a faulty link over an AP member port to other active links without affecting original data streams on these active links.

1.6.2 Restrictions and Guidelines

- Different disturbance factors may lead to the same disturbance effect.
- You can enable or disable the hash synchronization factors **ipv4**, **ipv6**, **fcoe**, and **on** as required.
- The flexible hash function can be configured in global configuration mode or interface configuration mode of a specific AP.
- Different products may support different load balancing algorithms.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the global load balancing algorithm of an AP.

aggregateport load-balance { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** | **src-dst-ip-l4port** | **enhanced profile** *profile-name* }

By default, for a device on which an AP is created as a L2 AP by default, load is distributed according to the source MAC addresses and destination MAC addresses of the incoming packets. For a device on which an AP is created as a L3 AP by default, load is distributed according to the source IP addresses and destination IP addresses of the incoming packets.

(4) (Optional) Rename the enhanced load balancing profile.

load-balance-profile *profile-name*

By default, if a device supports enhanced load balancing, the system creates a profile named **default** for enhanced load balancing. You can use this function to rename the profile or restore the default configurations.

(5) (Optional) Configure the load balancing mode of L2 packets.

l2 field { [**src-mac**] [**dst-mac**] [**src-port**] }

When the enhanced load balancing profile configuration is used as the flow balancing mode of AP, you can perform this configuration according to the traffic feature configuration of the network to implement better load balance.

The load balancing mode of L2 packets is a combination of **src-mac** and **dst-mac.**

(6) (Optional) Configure the load balancing mode of IPv4 packets.

ipv4 field { [**src-ip**] [**dst-ip**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**src-port**] }

Perform this configuration to specify the load balancing mode of IPv4 packets.

The load balancing mode of IPv4 packets is a combination of **src-ip**, **dst-ip**, **l4-src-port** and **l4-dst-port** by default.

(7) (Optional) Configure the load balancing mode of IPv6 packets.

ipv6 field { [**src-ip**] [**dst-ip**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**src-port**] }

Perform this configuration to specify the load balancing mode of IPv6 packets.

The load balancing mode of IPv6 packets is a combination of **src-ip**, **dst-ip**, **l4-src-port** and **l4-dst-port** by default.

(8) (Optional) Configure a hash disturbance factor.

hash-disturb { *factor-string* }

Perform this operation to balance packets of the same type over the AP for devices of the same type. It is not guaranteed that either configuration affects the balancing effect. If there is no expected effect, the other values can be configured.

The load balancing hash disturbance function is disabled by default.

(9) (Optional) Enable or disable hash synchronization.

hash-symmetrical { **ipv4** | **ipv6** }

Perform this operation to ensure that uplink and downlink streams of the same packet type are transmitted over the same path.

The hash synchronization function is disabled by default.

(10) (Optional) Configure the global load balance algorithm mode on an AP.

aggregateport algorithm mode *algorithm-number*

Perform this operation when the traffic model changes to keep optimal load balance.

The default algorithm mode is 11.

1.7 Configuring an AP Capacity Mode

1.7.1 Overview

- Change the maximum number of configurable APs and the maximum number of member ports in each AP.

1.7.2 Restrictions and Guidelines

- The system has a default AP capacity mode. You can run **show aggregateport capacity** to display the current capacity mode.
- If the current configuration (maximum number of APs or the number of member ports in each AP) exceeds the capacity to be configured, the capacity mode configuration will fail.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure an AP capacity mode.

aggregateport capacity mode *capacity-mode*

Perform this configuration to change the AP capacity, so as to meet the requirement imposed by changes in the number of APs in network deployment or the number of member ports that can be bound to each AP.

By default, up to 128 APs can be configured and each AP has up to 8 member ports.

1.8 Enabling BFD for AP Member Ports

1.8.1 Overview

- Enable BFD for all the member ports of a specified AP.
- After BFD is enabled for an AP, each member port performs BFD to determine whether the packets should be distributed to the member port for load balancing. When BFD detects a member port in **Down** state, the packets are not distributed to the port. When BFD detects that the member port is restored to **Up**, the packets are distributed to the port.

1.8.2 Restrictions and Guidelines

- After BFD is enabled for an AP, BFD sessions are set up. To make the sessions take effect, you need to configure BFD parameters. For details, see “Configuring BFD”.
- Enabling or disabling BFD for a single AP member port is not supported. You must enable or disable BFD for the entire AP group.
- Only member ports in forwarding state are enabled with BFD. If a member port is not in forwarding state because the link or LACP is **Down**, the BFD session on the member port is automatically deleted.
- If only one member port is available (that is, in forwarding state), all packets are distributed to this port. In this case, BFD fails. When there are more than one available member port, BFD takes effect again.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure BFD for AP member ports.

aggregate bfd-detect { **ipv4** *source-ipv4-address destination-ipv4-address* | **ipv6** *source-ipv6-address destination-ipv6-address* }

Enable BFD when you need to detect path failure on member ports in milliseconds. The flow on the faulty member port will be switched to other member port in case of link failure.

The BFD function of an AP member port is disabled by default.

1.9 Configuring a Preferred AP Member Port

1.9.1 Overview

- Configure a member port as the preferred AP member port.
- After the preferred member port is configured, the management VLAN packets on the AP are forwarded by this port.

1.9.2 Restrictions and Guidelines

- For details about management VLAN configuration, see “MAC VLAN” in “Configuring Ethernet Switching”.
- Only one preferred member port can be configured for one AP.
- After an LACP AP member port is configured as the preferred AP member port, if the LACP negotiation on all AP member ports fails, the preferred port is automatically downgraded to a static AP member port.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) (Optional) Configure a preferred AP member port.

aggregateport primary-port

Perform this configuration to specify an AP member port dedicated to forwarding management VLAN packets. The configuration is applicable to dual-system servers. Configure the port connected to the management NIC of the server as the preferred AP member port.

No preferred port is configured by default.

1.10 Configuring the Minimum Number of AP Member Ports

1.10.1 Overview

- After the minimum number of AP member ports is configured, the aggregation group takes effect only when the number of active member ports is greater than the minimum number.
- You can perform this operation to ensure that the link bandwidth provided by an AP aggregation group is greater than or equal to the sum of bandwidth provided by n AP member ports.
- After an action for the minimum number of AP member ports is configured, for example, shutting down the AP, the action is triggered when the number of AP member ports in **Up** state is less than the minimum number of the AP member ports.

1.10.2 Restrictions and Guidelines

- If the number of LACP AP member ports for an LACP aggregation group is less than the minimum number of AP member ports configured, all AP member ports are in the unbinding state, and the peer end is also automatically unbound.
- After the minimum number of static AP member ports is configured, if the number of static AP member ports in **Up** state is less than the minimum number, the static AP member ports in **Up** state cannot forward data and the corresponding AP is **Down**. However, the state of the peer end is not affected. Therefore, the corresponding functions need to be configured on the peer end.
- After an action for the minimum number of AP member port is configured, the action is triggered only when the number of AP member ports in **Up** state decreases to an insufficient number. For example, if the minimum number is set to 3, the action is triggered only when the number of AP member ports decreases from 3 or more to less than 3.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the AP configuration mode.

interface aggregateport *ap-number*

(4) (Optional) Configure the minimum number of AP member ports.

aggregateport member minimum { *port-number* | **action shutdown** }

Perform this configuration to specify the minimum number of the member ports of an AP aggregation group.

The minimum number of member ports of an AP is 1 by default.

(5) (Optional) Configure the action triggered when the number of AP member ports is smaller than the minimum value.

aggregateport member minimum { *port-number* | **action shutdown** }

Perform this configuration when some actions need to be triggered when the number of AP member ports in **Up** state is less than the minimum number of AP member ports.

By default, no action is configured for the minimum number of member ports in an AP.

1.11 Enabling the LACP Independent Port Function

1.11.1 Overview

- After the LACP independent port function is enabled, an LACP AP member port automatically changes to a common physical port if the LACP AP member port does not receive LACP packets within the set timeout period. The LACP AP member port state is changed to individual and the LACP AP member port can forward packets properly.
- After the LACP AP member port receives LACP packets, it changes to an LACP independent port again to perform LACP packet negotiation.
- The timeout period of an independent port can be adjusted by configuration.

1.11.2 Restrictions and Guidelines

- After the LACP independent port function is enabled, an LACP AP member port does not immediately change to a common physical port. Instead, the LACP AP member port changes to an independent port (a common physical port) only if it does not receive LACP packets within the set timeout period.
- The timeout period configuration of the LACP independent port only affects LACP AP member ports that have not changed into independent ports. After the timeout period is configured, the period calculation restarts.
- In long timeout mode, the LACP packet is sent every 30s. The timeout period should be longer than 30s so as not to affect the normal LACP negotiation. You are advised to configure the timeout period at least twice the period of LACP packet sending. In short timeout mode, the timeout period is not limited.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) (Optional) Enable the LACP independent port function.

lacp individual-port enable

Perform this operation so that an LACP AP member port can forward packets normally when the LACP AP member port cannot perform LACP negotiation.

The LACP independent port function is disabled by default.

(5) (Optional) Configure the timeout period of an LACP independent port.

lacp individual-timeout period *time*

Run this command to adjust the timeout period of an LACP independent port.

The timeout period of an LACP independent port is 90s by default.

1.12 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

You can run the **clear** commands to clear information.

Caution

- Running the **clear** command during operation of the device may lose vital information and interrupt services.
- System resources are occupied when debugging information is output. Therefore, disable the debugging function immediately after use.

Table 1-2 AP Monitoring

Command	Purpose
clear lacp counters [*key-number* | *interface-type interface-number*]	Clears the statistics of LACP packets on an LACP AP member port.
show load-balance-profile [*profile-name*]	Displays the configuration of the enhanced load balancing profile.
show lacp summary [*key-number*]	Displays the state of an LACP AP. You can view the information of a specified LACP AP by specifying **key-number**.
show lacp counters [*key-number*]	Displays the statistics of LACP packets on LACP AP member ports. You can view the information of a specified LACP AP by specifying **key-number**.
show aggregateport [*ap-number*] **summary**	Displays the summary of an AP.
show aggregateport load-balance	Displays the load balancing information of an AP.
show aggregateport capacity	Displays the capacity mode and usage of an AP.
debug lsm ap	Debugs an AP.
debug lacp { **cache-database** | **cli** | **ef-packet** | **threadld**| **pkt-agent** | **pkt-statis** | **pkt-thread** | **packet** | **event** | **ha** | **realtime** | **stm** | **timer** | **all** }	Debugs LACP.

1.13 Configuration Examples

1.13.1 Configuring Static APs

1. Requirements

Create AP interconnection for two devices on the IPv4 network, and configure static APs.

2. Topology

Figure 1-2 Topology for Configuring Static APs

3. Notes

- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static AP 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static AP 3.

4. Procedure

Create AP 3 on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3
```

Create AP 3 on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3
```

5. Verification

Run **show aggregateport summary** to check whether AP 3 contains member ports GigabitEthernet 0/1 and GigabitEthernet 0/2.

```
DeviceA# show aggregateport summary
AggregatePort MaxPorts SwitchPort Mode   Ports
------------- -------- ---------- ------ -----------------------------------
Ag3         8       Enabled   ACCESS Gi0/1,Gi0/2
DeviceB# show aggregateport summary
AggregatePort MaxPorts SwitchPort Mode   Ports
------------- -------- ---------- ------ -----------------------------------
Ag3         8       Enabled   ACCESS Gi0/1,Gi0/2
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 port-group 3
!
interface GigabitEthernet 0/2
 port-group 3
!
interface AggregatePort 3
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
 port-group 3
!
interface GigabitEthernet 0/2
 port-group 3
!
interface AggregatePort 3
!
```

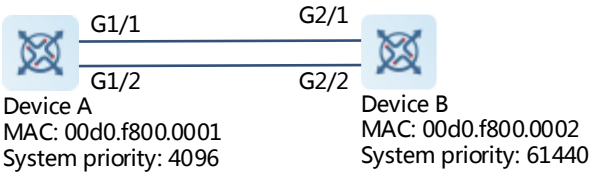
1.13.2 Configuring LACP APs

1. Requirements

Create AP interconnection for two devices on the IPv4 network, and configure dynamic APs.

2. Topology

Figure 1-3 Topology for Configuring LACP APs



3. Notes

- On Device A, set the LACP system priority to 4096.
- Enable dynamic link aggregation on the GigabitEthernet0/1 and GigabitEthernet0/2 ports on Device A and add the ports to LACP AP 3.
- On Device B, set the LACP system priority to 61440.
- Enable dynamic link aggregation on the GigabitEthernet0/1 and GigabitEthernet0/2 ports on Device B and add the ports to LACP AP 3.

4. Procedure

Configure LACP APs on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# lacp system-priority 4096
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# end
```

Configure LACP APs on Device B.

```
DevicB> enable
DeviceB# configure terminal
DeviceB(config)# lacp system-priority 61440
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3 mode active
```

5. Verification

Run **show lacp summary 3** to check whether LACP AP 3 contains member ports GigabitEthernet0/1 and GigabitEthernet0/2.

```
DeviceA# show LACP summary 3
System Id:32768,00d0.f8fb.0001
Flags:  S - Device is requesting Slow LACPDUs
 F - Device is requesting Fast LACPDUs.
A - Device is in active mode.       P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper    Port     Port
Port    Flags    State    Priority       Key    Number    State
--------------------------------------------------------------------
Gi0/1    SA       bndl       32768        0x3    0x1      0x3d
Gi0/2    SA       bndl       32768        0x3    0x2      0x3d
Partner information:
               LACP port               Oper    Port    Port
Port    Flags    Priority     Dev ID      Key    Number  State
-------------------------------------------------------------------
Gi0/1    SA       32768    00d0.f800.0002   0x3    0x1    0x3d
Gi0/2    SA       32768    00d0.f800.0002   0x3    0x2    0x3d
DeviceB # show LACP summary 3
SystemId:32768,00d0.f8fb.0002
Flags:  S - Device is requesting Slow LACPDUs
 F - Device is requesting Fast LACPDUs.
A - Device is in active mode.       P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper    Port     Port
Port    Flags    State    Priority       Key    Number    State
```

```
---------------------------------------------------------------------
Gi0/1    SA       bndl       32768        0x3    0x1      0x3d
Gi0/2    SA       bndl       32768        0x3    0x2      0x3d
Partner information:
               LACP port               Oper    Port    Port
Port    Flags    Priority     Dev ID      Key    Number  State
--------------------------------------------------------------------
Gi0/1    SA       32768    00d0.f800.0001   0x3    0x1    0x3d
Gi0/2    SA       32768    00d0.f800.0001   0x3    0x2    0x3d
```

6. Configuration Files

- Device A configuration file

```
!
lacp system-priority 4096
!
interface GigabitEthernet 0/1
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 port-group 3 mode active
!
interface AggregatePort 3
!
```

- Device B configuration file

```
!
lacp system-priority 61440
!
interface GigabitEthernet 0/1
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 port-group 3 mode active
!
interface AggregatePort 3
!
```

1.13.3 Enabling LinkTrap

1. Requirements

On the IPv4 network, create AP interconnection for two devices, configure static APs, and enable LinkTrap.

2. Topology

Figure 1-4 Topology for Enabling LinkTrap

3. Notes

- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static AP 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static AP 3.
- On Device A, disable LinkTrap for AP 3 and enable LinkTrap for its AP member ports.
- On Device B, disable LinkTrap for AP 3 and enable LinkTrap for its AP member ports.

4. Procedure

Perform the following configuration on Device A.

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3
DeviceA(config-if-range)# exit
DeviceA(config)# aggregateport member linktrap
DeviceA(config)# interface Aggregateport 3
DeviceA(config-if-AggregatePort 3)# no snmp trap link-status
```

Perform the following configuration on Device B:

```
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3
DeviceB(config-if-range)# exit
DeviceB(config)# aggregateport member linktrap
DeviceB(config)# interface Aggregateport 3
DeviceB(config-if-AggregatePort 3)# no snmp trap link-status
```

5. Verification

Run **show running** to check whether LinkTrap is enabled for AP 3 and its member ports.

```
DeviceA# show run | include AggregatePort 3
Building configuration...
Current configuration: 54 bytes
interface AggregatePort 3
 no snmp trap link-status
DeviceA# show run | include AggregatePort
aggregateport member linktrap
```

```
DeviceB# show run | include AggregatePort 3
Building configuration...
Current configuration: 54 bytes
interface AggregatePort 3
 no snmp trap link-status
DeviceB# show run | include AggregatePort
aggregateport member linktrap
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 port-group 3
!
interface GigabitEthernet 0/2
 port-group 3
!
interface AggregatePort 3
 no snmp trap link-status
!
aggregateport member linktrap
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 port-group 3 mode active
!
interface AggregatePort 3
 no snmp trap link-status
!
aggregateport member linktrap
!
```

1.13.4 Configuring a Load Balancing Mode

1. Requirements

On the IPv4 network, create AP interconnection for two devices, configure static APs, and enable load balancing.

2. Topology

Figure 1-5 Topology for Configuring a Load Balancing Mode Topology

3. Notes

- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static AP 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static AP 3.
- On Device A, configure source MAC address-based load balancing for AP 3 in global configuration mode.
- On Device B, configure destination MAC address-based load balancing for AP 3 in global configuration mode.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3
DeviceA(config-if-range)# exit
DeviceA(config)# aggregateport load-balance src-mac
```

Perform the following configuration on Device B:

```
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3
DeviceB(config-if-range)# exit
DeviceB(config)# aggregateport load-balance dst-mac
```

5. Verification

Run **show aggregateport load-balance** to check the load balancing algorithm configuration.

```
DeviceA   # show aggregatePort load-balance
Load-balance   : Source MAC
```

```
DeviceB   # show aggregatePort load-balance
Load-balance   : Destination MAC
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 port-group 3
```

```
!
interface GigabitEthernet 0/2
 port-group 3
!
interface AggregatePort 3
!
aggregateport load-balance src-mac
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
 port-group 3
!
interface GigabitEthernet 0/2
 port-group 3
!
interface AggregatePort 3
!
aggregateport load-balance dst-mac
!
```

7. Common Errors

A user configures the factors **ipv4**, **ipv6**, **fcoe**, and **on** for enabling hash synchronization. However, no configuration is displayed when the user runs **show running**. This is because hash synchronization is enabled for some products by default. The configuration will be displayed after the user disables the function.

1.13.5 Configuring Hash Load Balancing Control

1. Requirements

Create AP interconnection for two devices on the IPv4 network.

2. Topology

Figure 1-6 Topology for Configuring Static APs

3. Notes

- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static AP 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static AP 3.
- On Device A, disable hash synchronization for IPv4 packets.
- On Device B, disable hash synchronization for IPv4 packets.

- On Device A, configure the hash disturbance factor A.
- On Device B, configure the hash disturbance factor B.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3
DeviceA(config-if-range)# exit
DeviceA(config)# load-balance-profile default
DeviceA(config-load-balance-profile)# no hash-symmetrical ipv4
DeviceA(config-load-balance-profile)# hash-disturb A
DeviceA(config-load-balance-profile)# exit
```

Perform the following configuration on Device B:

```
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3
DeviceB(config-if-range)# exit
DeviceB(config)# load-balance-profile default
DeviceB(config-load-balance-profile)# no hash-symmetrical ipv4
DeviceA(config-load-balance-profile)# hash-disturb B
DeviceB(config-load-balance-profile)# exit
```

5. Verification

Run **show running** to check whether the configuration is correct.

6. Configuration Files

- Device A configuration file

```
!
load-balance-profile default
 no hash-symmetrical ipv4
 hash-disturb A
!
interface GigabitEthernet 0/1
 port-group 3
!
interface GigabitEthernet 0/2
 port-group 3
!
```

- Device B configuration file

```
!
load-balance-profile default
 no hash-symmetrical ipv4
 hash-disturb B
```

```
!
interface GigabitEthernet 0/1
 port-group 3
!
interface GigabitEthernet 0/2
 port-group 3
!
```

7. Common Errors

A user configures the factors **ipv4**, **ipv6** and **on** for enabling hash synchronization. However, no configuration is displayed when the user runs **show running**. This is because hash synchronization is enabled for some products by default. The configuration will be displayed after the user disables the function.

1.13.6 Configuring an AP Capacity Mode

1. Requirements

Create AP interconnection for two devices on the IPv4 network.

2. Topology

Figure 1-7 Configuring an AP Capacity Mode

3. Notes

- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static AP 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static AP 3.
- On Device A, configure the 128 x 128 AP capacity mode.
- On Device B, configure the 256 x 64 AP capacity mode.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3
DeviceA(config-if-range)# exit
DeviceA(config)# aggregateport capacity mode 128*8
```

Perform the following configuration on Device B:

```
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3
DeviceB(config-if-range)# exit
```

```
DeviceB(config)# aggregateport capacity mode 128*8
```

5. Verification

Run **show aggregateport capacity** to check the AP capacity mode configuration.

```
DeviceA# show aggregatePort capacity
AggregatePort Capacity Information:
Configuration Capacity Mode: 128*8.
Effective Capacity Mode   : 128*8.
Available Capacity Mode   : 128*8.
Total Number : 128, Used: 1, Available: 127.
DeviceB  DeviceB# show aggregatePort capacity
AggregatePort Capacity Information:
Configuration Capacity Mode: 256*64.
Effective Capacity Mode   : 256*64.
Available Capacity Mode   : 256*64.
Total Number : 256, Used: 1, Available: 255.
```

6. Configuration Files

- Device A configuration file

```
!
aggregateport capacity mode 128*8
!
interface GigabitEthernet 0/1
 port-group 3
!
interface GigabitEthernet 0/2
 port-group 3
!
```

- Device B configuration file

```
!
aggregateport capacity mode 128*8
!
interface GigabitEthernet 0/1
 port-group 3
!
interface GigabitEthernet 0/2
 port-group 3
!
interface AggregatePort 3
!
```

1.13.7 Enabling BFD for Member Ports

1. Requirements

Create AP interconnection for two devices on the IPv4 network.

2. Topology

Figure 1-8 Topology for Enabling BFD for AP Member Ports

3. Notes

- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A and add the ports to LACP AP 3.
- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B and add the ports to LACP AP 3.
- Configure IP address 1.0.0.1 for AP 3 on Device A and enable IPv4 BFD.
- Configure IP address 1.0.0.2 for AP 3 on Device B and enable IPv4 BFD.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# no switchport
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# exit
DeviceA(config)# interface aggregateport 3
DeviceA(config-if-Aggregateport 3)# ip address 1.0.0.1 255.255.255.0
DeviceA(config-if-Aggregateport 3)# aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2
DeviceA(config-if-Aggregateport 3)# bfd interval 50 min_rx 50 multiplier 3
```

Perform the following configuration on Device B:

```
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# no switchport
DeviceB(config-if-range)# port-group 3 mode active
DeviceB(config-if-range)# exit
DeviceB(config)# interface aggregateport 3
DeviceB(config-if-Aggregateport 3)# ip address 1.0.0.2 255.255.255.0
DeviceB(config-if-Aggregateport 3)# aggregate bfd-detect ipv4 1.0.0.2 1.0.0.1
DeviceB(config-if-Aggregateport 3)# bfd interval 50 min_rx 50 multiplier 3
```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show interface aggregateport** to view the BFD state of each AP member port.

```
DeviceA# show run | include AggregatePort 3
Building configuration…
```

```
Current configuration: 54 bytes
interface AggregatePort 3
 no switchport
 ip address 1.0.0.1 255.255.255.0
 aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2
 bfd interval 50 min_rx 50 multiplier 3
DeviceA# show interface aggregateport 3
…
Aggregate Port Informations:
       Aggregate Number: 3
       Nam“: “AggregatePor” 3"
       Members: (count=2)
       GigabitEthernet 0/1       Link Status: Up   Lacp Status: bndl   BFD Status:
UP
       GigabitEthernet 0/2       Link Status: Up   Lacp Status: bndl   BFD Status:
UP
```

```
DeviceB# show run | include AggregatePort 3
Building configuration...
Current configuration: 54 bytes
interface AggregatePort 3
 no switchport
 ip address 1.0.0.2 255.255.255.0
 aggregate bfd-detect ipv4 1.0.0.2 1.0.0.1
 bfd interval 50 min_rx 50 multiplier 3
DeviceB# show interface aggregateport 3
…
Aggregate Port Informations:
       Aggregate Number: 3
       Nam“: "AggregatePor” 3"
       Members: (count=2)
       GigabitEthernet 0/1       Link Status: Up   Lacp Status: bndl   BFD Status:
UP
       GigabitEthernet 0/2       Link Status: Up   Lacp Status: bndl   BFD Status:
UP
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 no switchport
```

```
 port-group 3 mode active
!
interface AggregatePort 3
 no switchport
 aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2
 ip address 1.0.0.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 no switchport
 port-group 3 mode active
!
interface AggregatePort 3
 no switchport
 aggregate bfd-detect ipv4 1.0.0.2 1.0.0.1
 ip address 1.0.0.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
```

7. Common Errors

- If BFD is enabled for an AP without BFD parameters, BFD does not take effect.
- After BFD is enabled for an AP, the BFD neighbor must be a directly connected AP enabled with BFD.

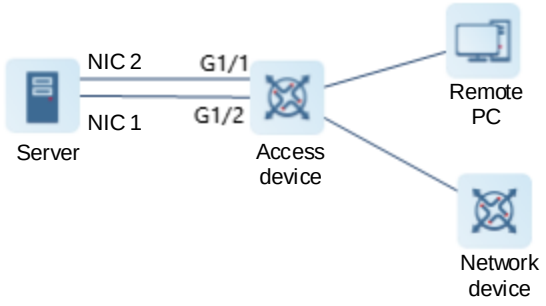
1.13.8 Configuring Interworking Between the Access Device and a Server with Two NICs over a Preferred LACP AP

1. Requirements

The server has two management systems: the remote management OS and server OS. The two OSs are independent of each other. When the server OS restarts, access to the remote management OS is normal. The remote management OS is used to manage the server OS and uses NIC 1 as the communication port to access the access device GigabitEthernet0/1 in Figure 1-9. It is allocated with a specific VLAN, for example, VLAN 10. The server OS is used to handle routine production services and uses NIC 1 and NIC 2 as the communication ports. LACP aggregation is enabled between NIC 1 and NIC 2. The server OS accesses the access device over the aggregate link. A VLAN except the management VLAN is allocated to the server OS. NIC 1 is used as the communication port for both the remote management OS and server OS. Based on the VLAN tag carried in packets, the server determines whether packets received from NIC 1 are sent to the remote management OS or server OS.

2. Topology

Figure 1-9 Topology for Configuring Interworking Between the Access Device and a Server with Two NICs over a Preferred LACP AP



3. Notes

- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on the access device and add the ports to LACP AP 3.
- Configure GigabitEthernet 0/1 on the access device as the preferred port.
- Configure VLAN 10 on the access device as the management VLAN.

4. Procedure

Create LACP AP 3 and add AP 3 to the trunk.

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# exit
DeviceA(config)# interface aggregateport 3
DeviceA(config-if-Aggregateport 3)# switchport mode trunk
DeviceA(config-if-Aggregateport 3)# exit
```

Configure VLAN 10 as the management VLAN.

```
DeviceA(config)# aggregateport-admin vlan 10
```

Configure GigabitEthernet 0/1 as the preferred port.

```
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1) aggregateport primary-port
```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show interface aggregateport** to query the preferred AP member port.

```
DeviceA# show run | include aggregateport-admin
Building configuration...
Current configuration: 54 bytes
aggregateport-admin vlan 10
DeviceA# show run | include GigabitEthernet 0/1
Building configuration...
```

```
Current configuration: 54 bytes
interface GigabitEthernet 0/1
aggregateport primary-port
 portgroup 3 mode active
DeviceA# show interface aggregateport 3
…
Aggregate Port Informations:
       Aggregate Number: 3
       Nam": "AggregatePor" 3"
       Members: (count=2)
      Primary Port: GigabitEthernet 0/1
       GigabitEthernet 0/1        Link Status: Up    Lacp Status: bndl
       GigabitEthernet 0/2        Link Status: Up    Lacp Status: bndl
  …
```

6. Configuration Files

- Device A configuration file

```
!
aggregateport-admin vlan 10
!
interface GigabitEthernet 0/1
 port-group 3 mode active
 aggregateport primary-port
!
interface GigabitEthernet 0/2
 port-group 3 mode active
!
interface AggregatePort 3
 switchport mode trunk
!
```

1.13.9 Configuring Automatic Server Deployment over a Preferred LACP AP

1. Requirements

The server has two NICs, and the two NICs connect to Switch A over the LACP AP. The server can be automatically installed over NIC 1. After the server is installed, management data streams are sent over NIC 1 and NIC 2 for mutual backup and load balancing.

2. Topology

Figure 1-10 Topology for Configuring Automatic Server Deployment over a Preferred LACP AP

3. Notes

- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A and add the ports to LACP AP 3.
- Configure GigabitEthernet 0/1 on Device A as the preferred port.

4. Procedure

Create LACP AP 3.

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# exit
```

Configure GigabitEthernet 0/1 as the preferred port.

```
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1) aggregateport primary-port
```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show interface aggregateport** to query the preferred AP member port.

```
DeviceA# show run | include GigabitEthernet 0/1
Building configuration...
Current configuration: 54 bytes
interface GigabitEthernet 0/1
aggregateport primary-port
 portgroup 3 mode active
DeviceA# show interface aggregateport 3
…
Aggregate Port Informations:
       Aggregate Number: 3
       Nam“: "AggregatePor” 3"
       Members: (count=2)
      Primary Port: GigabitEthernet 0/1
       GigabitEthernet 0/1       Link Status: Up   Lacp Status: bndl
       GigabitEthernet 0/2       Link Status: Up   Lacp Status: bndl
  …
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 port-group 3 mode active
 aggregateport primary-port
!
interface GigabitEthernet 0/2
 port-group 3 mode active
```

```
!
interface AggregatePort 3
!
```

1.13.10 Configuring the Minimum Number of AP Member Ports (When the Number of AP Member Ports Is Less Than the Minimum Number)

1. Requirements

On the IPv4 network, create AP interconnection for two devices, and configure a number of AP member ports less than the minimum number of AP Member ports.

2. Topology

Figure 1-11 Topology for Configuring the Minimum Number of AP Member Ports

3. Notes

- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A and add the ports to LACP AP 3.
- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet0/2 ports on Device B and add the ports to LACP AP 3.
- On Device A, set the minimum number of the member ports of AP 3 to 3.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# no switchport
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# exit
DeviceA(config)# interface aggregateport 3
DeviceA(config-if-Aggregateport 3)# aggregateport member minimum 3
```

Perform the following configuration on Device B:

```
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# no switchport
DeviceB(config-if-range)# port-group 3 mode active
DeviceB(config-if-range)# exit
DeviceB(config)# interface aggregateport 3
DeviceB(config-if-Aggregateport 3)# aggregateport member minimum 3
```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show lacp summery** to view the aggregation state of each AP member port.

```
DeviceA# show LACP summary 3
System Id:32768, 00d0.f8fb.0001
Flags: -S - Device is requesting Slow LACPDUs
-F - Device is requesting Fast LACPDUs.-A - Device is in active mode.      -P - Device
is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper    Port     Port
Port    Flags    State    Priority       Key    Number   Sta--
Gi0/1    SA       susp       32768        0x3    0x1      0x3d
Gi0/2    SA       susp       32768        0x3    0x2      0x3d
Partner information:
                LACP port               Oper    Port    Port
Port    Flags    Priority     Dev ID      Key    Number  Sta--
Gi0/1    SA       32768    00d0.f800.0002  0x3    0x1    0x3d
Gi0/2    SA       32768    00d0.f800.0002  0x3    0x2    0x3d
```

6. Configuration Files

- Configuration file of device A

```
!
interface GigabitEthernet 0/1
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 no switchport
 port-group 3 mode active
!
interface AggregatePort 3
 no switchport
 aggregateport member minimum 3
!
```

- Configuration file of Device B

```
!
interface GigabitEthernet 0/1
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 no switchport
 port-group 3 mode active
```

```
!
interface AggregatePort 3
 no switchport
 aggregateport member minimum 3
!
```

1.13.11 Configuring the Minimum Number of AP Member Ports (When the Number of AP Member Ports Is Not Less Than the Minimum Number)

1. Requirements

On the IPv4 network, create AP interconnection for two devices, and configure the number of AP member ports not less than the minimum number of AP Member ports.

2. Topology

Figure 1-12 Topology for Configuring the Minimum Number of AP Member Ports

3. Notes

- Enable LACP for the GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3 ports on Device A and add the ports to LACP AP 3.
- Enable LACP for the GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3 ports on Device B and add the ports to LACP AP 3.
- On Device A, set the minimum number of member ports of AP 3 to 2.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-3
DeviceA(config-if-range)# no switchport
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# exit
DeviceA(config)# interface aggregateport 3
DeviceA(config-if-Aggregateport 3)# aggregateport member minimum 2
```

Perform the following configuration on Device B:

```
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-3
DeviceB(config-if-range)# no switchport
DeviceB(config-if-range)# port-group 3 mode active
DeviceB(config-if-range)# exit
DeviceB(config)# interface aggregateport 3
```

```
DeviceB(config-if-Aggregateport 3)# aggregateport member minimum 2
```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show lacp summery** to view the aggregation state of each AP member port.

```
DeviceA# show LACP summary 3
System Id:32768,00d0.f8fb.0001
Flags: -S - Device is requesting Slow LACPDUs
-F - Device is requesting Fast LACPDUs.-A - Device is in active mode.      -P - Device
is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper    Port     Port
Port    Flags    State    Priority       Key    Number   Sta--
Gi0/1    SA       bndl       32768        0x3    0x1      0x3d
Gi0/2    SA       bndl       32768        0x3    0x2      0x3d
Gi0/3    SA       bndl       32768        0x3    0x3      0x3d

Partner information:
                LACP port               Oper    Port    Port
Port    Flags    Priority     Dev ID      Key    Number  Sta--
Gi0/1    SA       32768    00d0.f800.0002  0x3    0x1    0x3d
Gi0/2    SA       32768    00d0.f800.0002  0x3    0x2    0x3d
Gi0/3    SA       32768    00d0.f800.0002  0x3    0x3    0x3d
```

6. Configuration Files

- Configuration file of device A

```
!
interface GigabitEthernet 0/1
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/3
 no switchport
 port-group 3 mode active
!
interface AggregatePort 3
 no switchport
 aggregateport member minimum 2
!
```

- Configuration file of device A

```
!
interface GigabitEthernet 0/1
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/3
 no switchport
 port-group 3 mode active
!
interface AggregatePort 3
 no switchport
 aggregateport member minimum 2
!
```

1.13.12 Enabling the LACP Independent Port Function

1. Requirements

The server uses NIC 1 and NIC 2 as the communication ports to get access to the GigabitEthernet0/1 and GigabitEthernet0/2 of the access device. GigabitEthernet0/1 and GigabitEthernet0/2 are added to the LACP aggregation group, for example, AP 3. A specific VLAN, for example, VLAN 10 is allocated. The LACP independent port function is enabled for GigabitEthernet0/1 and GigabitEthernet0/2. When the OS is not installed on the server, LACP negotiation between the server and the access device fails. In this case, GigabitEthernet0/1 and GigabitEthernet0/2 of the access device change to common physical ports and are allocated to VLAN 10 automatically. The server uses NIC 1 or NIC 2 to communicate with the remote OS installation device. After the OS is installed, the server connects to the access device in LACP mode.

2. Topology

Figure 1-13 Topology for Enabling the LACP Independent Port Function

3. Notes

- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on the access device and add the ports to LACP AP 3.
- Enable the LACP independent port function for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on the access device.
- Allocate AP 3 on the access device to VLAN 10.

4. Procedure

Create an AP on Device A.

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# lacp individual-port enable
DeviceA(config-if-range)# exit
DeviceA(config)# interface aggregateport 3
DeviceA(config-if-Aggregateport 3)# switch access vlan 10
```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show lacp summery** to view the aggregation state of each AP member port.

```
DeviceA# show LACP summary 3
System Id:32768,00d0.f8fb.0001
Flags: -S - Device is requesting Slow LACPDUs
-F - Device is requesting Fast LACPDUs.-A - Device is in active mode.      -P - Device
is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper    Port     Port
Port    Flags    State    Priority       Key    Number    Sta--
Gi0/1    SA       individual    32768        0x3    0x1      0x3d
Gi0/2    SA       individual    32768        0x3    0x2      0x3d
Partner information:
               LACP port               Oper    Port    Port
Port    Flags    Priority     Dev ID      Key    Number  Sta--
Gi0/1    SA       32768    00d0.f800.0002   0x3    0x1    0x3d
Gi0/2    SA       32768    00d0.f800.0002   0x3    0x2    0x3d
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 port-group 3 mode active
 lacp individual-port enable
!
interface GigabitEthernet 0/2
 port-group 3 mode active
 lacp individual-port enable
!
interface AggregatePort 3
 switchport access vlan 10
!
```

Ethernet Switching Configuration

1. MAC Address Configuration
2. MAC Loopback Configuration
3. VLAN Configuration
4. Private VLAN Configuration
5. Super VLAN Configuration
6. Voice VLAN Configuration
7. GVRP Configuration
8. QinQ Configuration
9. MSTP Configuration
10. ERPS Configuration
11. LLDP Configuration

Contents

1 Configuring MAC Address 1
1.1 Introduction 1
1.1.1 MAC Address Table 1
1.1.2 Classification of MAC Address Entries 1
1.1.3 Generation of MAC Address Entries 1
1.1.4 Update and Aging of MAC Address Entries 3
1.1.5 Protocols and Standards 3
1.2 Restrictions and Guidelines 4
1.3 Configuration Task Summary 4
1.4 Configuring Static MAC Address Entries 4
1.4.1 Overview 4
1.4.2 Restrictions and Guidelines 4
1.4.3 Procedure 4
1.5 Configuring Filtering MAC Address Entries 5
1.5.1 Overview 5
1.5.2 Procedure 5
1.6 Disabling Dynamic MAC Address Learning 5
1.6.1 Overview 5
1.6.2 Disabling MAC Address Learning in Global Configuration Mode 5
1.6.3 Disabling MAC Address Learning for an Interface 6
1.7 Configuring Upper Limit of Learned MAC Addresses 6
1.7.1 Overview 6

1.7.2 Configuring Upper Limit of MAC Addresses Learned from a VLAN.....6

1.7.3 Configuring Upper Limit of MAC Addresses Learned from an Interface.....7

1.8 Configuring Aging Time of Dynamic MAC Address Entries.....8

1.9 Enabling MAC Address Flapping Detection and Protection.....8

1.9.1 Overview.....8

1.9.2 Procedure.....8

1.10 Configuring Reporting Interval of MAC Address Table Usage Alarms and MAC Address Table Usage Threshold.....9

1.10.1 Overview.....9

1.10.2 Procedure.....9

1.11 Configuring the Function of MAC Address Entry Change Notification.....10

1.11.1 Overview.....10

1.11.2 Restrictions and Guidelines.....10

1.11.3 Procedure.....10

1.12 Monitoring.....11

1.13 Configuration Examples.....12

1.13.1 Configuring MAC Address Flapping Detection.....12

1.13.2 Configuring the Function of MAC Address Change Notification.....14

1 Configuring MAC Address

1.1 Introduction

A Media Access Control (MAC) address is used to identify the position of a device in a network. Generally, a MAC address consists of 12 hexadecimals and contains a total of 48 bits (six bytes). The first 24 bits are applied for by vendors from The Internet Engineering Task Force (IETF) and used to identify a network device manufacturer. The last 24 bits are assigned by the vendors and used to identify network cards produced by the manufacturers.

1.1.1 MAC Address Table

A MAC address table records mappings of MAC addresses and interfaces to virtual local area networks (VLANs). A device queries the MAC address table based on the destination MAC address in a received packet. If the device finds an entry that is consistent with the destination MAC Address in the packet, the device forwards the packet through the interface corresponding to the entry in unicast mode. If the device does not find such an entry, it forwards the packet through all interfaces other than the receiving interface in broadcast mode.

Note

This section describes static, dynamic, and filtering MAC address entries. For more information about multicast MAC address entries and specific configurations, see "IGMP" in *Multicast Configuration Guide*.

1.1.2 Classification of MAC Address Entries

MAC address entries are classified into the following types:

- Static MAC address entries: Manually configured by the administrator. Packets whose destination MAC address matches the one in such an entry are forwarded through the correct interface. This type of entries does not age.
- Dynamic MAC address entries: Automatically generated by devices. Packets whose destination MAC address matches the one in such an entry are forwarded through the correct interface. This type of entries ages.
- Filtering MAC address entries: Manually configured by the administrator. Packets whose source or destination MAC address matches the one in such an entry are discarded. This type of entries does not age.

The priorities of these types of MAC address entries are ranked in descending order as follows: Filtering MAC address entries > Static MAC address entries > Dynamic MAC address entries. If two entries have the same MAC address and VLAN, the higher-priority entry can overwrite the lower-priority one, and entries with the same priority can overwrite each other.

1.1.3 Generation of MAC Address Entries

A MAC address entry can be automatically learned or manually configured.

1. Automatic learning

A device automatically generates a MAC address entry based on the source MAC address in a received packet. The learning procedure is as follows:

(1) Initially, the MAC address table of Device A is empty. To send a packet to User C, User A sends the packet to the interface GigabitEthernet 0/1 of Device A. Upon receiving the packet, Device A generates a MAC address entry, with the MAC address being MAC A and the interface being GigabitEthernet 0/1.

(2) As Device A does not have an entry corresponding to MAC A, it forwards the packet through all interfaces other than GigabitEthernet 0/1 in broadcast mode. In this case, other users also receive the packet that User A sends to User C.

(3) User C sends a reply packet destined for User A to Device A through the interface GigabitEthernet 0/3. Upon receiving the packet, Device A generates a MAC address entry, with the MAC address being MAC C and the interface being GigabitEthernet 0/3. Meanwhile, Device A finds an entry corresponding to MAC A and then forwards the packet to User A through GigabitEthernet 0/1 in unicast mode.

(4) After the communication between User A and User C is complete, Device A learns two MAC address entries. Later, packets are forwarded between User A and User C in unicast mode and other users do not receive packets destined for these two users.

Figure 1-1 Automatically Learning MAC Address Entry I

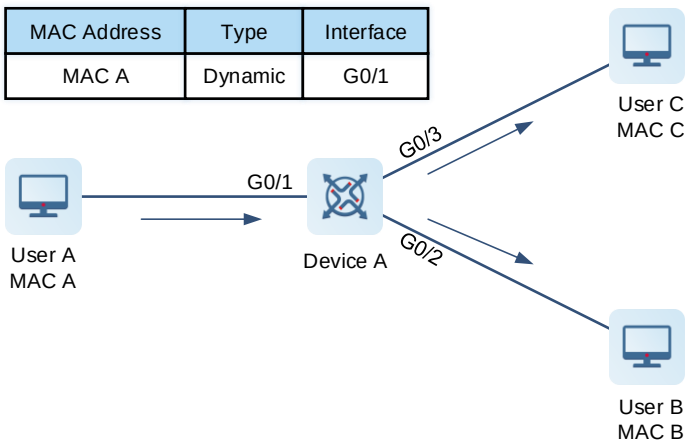
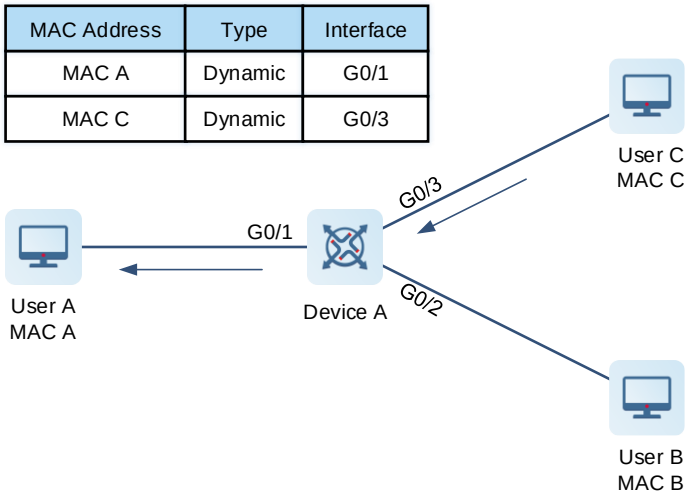


Figure 1-2 Automatically Learning MAC Address Entry II



2. Manual configuration

If the device forwards packets based on automatically generated MAC address entries, security risks exist. For example, if an attacker forges a packet by using a MAC address of a valid user and sends the packet to another interface of the device, the device automatically updates the corresponding MAC address entry and sends subsequent packets destined for the user to the attacker. To improve network security, the network administrator can add a specified MAC address entry to bind the MAC address of the valid user to a device interface. The static MAC address entry configured in this way is not updated due to packet forwarding. If a packet whose source MAC address is the MAC address of the valid user is received from another user, the device directly discards this packet.

1.1.4 Update and Aging of MAC Address Entries

Static and filtering MAC address entries do not automatically update or age. Dynamic MAC address entries are updated and age in the following scenarios:

(1) When the device learns a new dynamic MAC address entry, the device sets the age flag bit of this entry to 1.

(2) If the source MAC address in a received packet already exists in the MAC address table, the device updates the entry and sets the age flag bit to 1.

(3) The device checks the age flag bit of a dynamic MAC address entry at the interval of the aging time. For entries whose flag bit is 1, the device sets the flag bit to 0. For entries whose flag bit is 0, the device deletes the entries.

Therefore, the actual aging time of a dynamic MAC address entry ranges between the specified age value and two times the age value.

1.1.5 Protocols and Standards

- IEEE 802.3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications
- IEEE 802.1Q: Virtual Bridged Local Area Networks

1.2 Restrictions and Guidelines

If an L2 interface has subinterfaces, running the **default interface** command in global configuration mode does not affect configurations related to the MAC address learning function, the upper limit of learned MAC addresses, the forwarding rule to be used after the upper limit of learned MAC addresses is reached, and the MAC address flapping protection policy.

1.3 Configuration Task Summary

All the following configuration tasks are optional and may be selected as needed.

- Configuring Static MAC Address Entries
- Configuring Filtering MAC Address Entries
- Disabling Dynamic MAC Address Learning
  - Disabling MAC Address Learning in Global Configuration Mode
  - Disabling MAC Address Learning for an Interface
- Configuring Upper Limit of Learned MAC Addresses
  - Configuring Upper Limit of MAC Addresses Learned from a VLAN
  - Configuring Upper Limit of MAC Addresses Learned from an Interface
- Configuring Aging Time of Dynamic MAC Address Entries
- Enabling MAC Address Flapping Detection and Protection
- Configuring Reporting Interval of MAC Address Table Usage Alarms and MAC Address Table Usage Threshold
- Configuring the Function of MAC Address Entry Change Notification

1.4 Configuring Static MAC Address Entries

1.4.1 Overview

You can manually configure static MAC address entries to bind MAC addresses to device interfaces.

1.4.2 Restrictions and Guidelines

- Interfaces in the MAC address entries can be specified as L2 Ethernet interfaces or L2 aggregation ports (APs).
- If a MAC address is bound to different interfaces in the same VLAN, the last configuration prevails.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static MAC address.

mac-address-table static *mac-address* **vlan** *vlan-id* **interface** *interface-type interface-number*

No static MAC address entry exists by default.

1.5 Configuring Filtering MAC Address Entries

1.5.1 Overview

To prohibit a user from sending and receiving packets in certain scenarios, you can add the MAC address of the user to a filtering MAC address entry. After the entry is configured, packets whose source or destination MAC address matches the MAC address in the filtering MAC address entry are directly discarded.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a filtering MAC address.

mac-address-table filtering *mac-address* **vlan** *vlan-id*

No filtering MAC address entry exists by default.

1.6 Disabling Dynamic MAC Address Learning

1.6.1 Overview

MAC address learning is enabled by default. A device automatically generates a dynamic MAC address entry based on the source MAC address in a received packet. The device queries the MAC address table to perform unicast forwarding, which reduces broadcast frequency and therefore reduces the network traffic. The device learns or updates the MAC address entry each time it receives a packet, which results in low security. An attacker may forge and send a large number of packets with different source MAC addresses to the device to use up the MAC address entry resources. Consequently, the device cannot update the MAC address entries in time. You can disable dynamic MAC address learning if required.

1.6.2 Disabling MAC Address Learning in Global Configuration Mode

1. Overview

If you disable MAC address learning in global configuration mode, the device does not learn MAC addresses.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable MAC address learning in global configuration mode.

mac-address-learning disable

MAC address learning is enabled in global configuration mode by default.

1.6.3 Disabling MAC Address Learning for an Interface

1. Overview

If MAC address learning is enabled in global configuration mode, you can disable this function for a specific interface.

2. Restrictions and Guidelines

- If 802.1X, IP Source Guard, or the port security function is configured on an interface, MAC address learning must be disabled for this interface. For more information about 802.1X, IP Source Guard, or the port security function, see sections "802.1X", "IP Source Guard", or "Port Security" in *Security Configuration Guide*.
- This function can be enabled on L2 Ethernet interfaces and L2 APs only.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(1) Enter the global configuration mode.

configure terminal

(2) Enter the interface configuration mode.

interface *interface-type interface-number*

(3) Disable MAC address learning for an interface.

no mac-address-learning

No MAC address learning is enabled for an interface by default.

1.7 Configuring Upper Limit of Learned MAC Addresses

1.7.1 Overview

The number of MAC address entries on the device is limited. Packets can be forwarded only in broadcast mode in order to prevent the device from learning a large number of dynamic MAC address entries from an interface or a VLAN (for example, when it is attacked by packets with different source addresses) and prevent MAC address learning failures on other interfaces and VLANs. In this case, you can configure the upper limit of MAC addresses learned from each interface or VLAN based on actual network plans. When the number of MAC addresses reaches the upper limit, the device stops learning MAC addresses from the corresponding interface or VLAN. You can also configure a forwarding rule to be used after the number of learned MAC addresses reaches the upper limit, to determine whether to forward packets whose source MAC address is not in the MAC address table. With this function, you can save MAC address entry resources and enhance network security.

This function is available only to dynamic MAC address entries.

1.7.2 Configuring Upper Limit of MAC Addresses Learned from a VLAN

1. Overview

You can configure the upper limit of MAC addresses learned from a VLAN and the packet forwarding rule to be used after the number of learned MAC addresses reaches the upper limit.

2. Restrictions and Guidelines

- If the number of MAC addresses learned from a VLAN is greater than the upper limit, the device stops learning MAC addresses from the VLAN, and starts learning again only after the number drops below the upper limit as aged address entries are deleted.
- This function does not limit replication of MAC address entries to a VLAN whose number of learned MAC address entries reaches the upper limit.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a VLAN and enter the VLAN configuration mode.

vlan *vlan-id*

(4) Configure the upper limit of dynamic MAC addresses learned from a VLAN.

max-dynamic-mac-count *count*

No upper limit of learned MAC addresses is configured for a VLAN by default.

(5) (Optional) Configure a forwarding rule to be used after the number of dynamic MAC addresses learned from a VLAN reaches the upper limit.

max-dynamic-mac-count exceed-action { **forward** | **discard** }

By default, after the number of MAC addresses learned from a VLAN reaches the upper limit, the device continues forwarding packets whose source MAC address is not learned.

1.7.3 Configuring Upper Limit of MAC Addresses Learned from an Interface

1. Overview

You can configure the upper limit of MAC addresses learned from an interface and the packet forwarding rule to be used after the number of learned MAC addresses reaches the upper limit.

2. Restrictions and Guidelines

If the number of MAC addresses learned from an interface is greater than the upper limit, the device stops learning MAC addresses from the interface, and starts learning again only after the number drops below the upper limit as aged MAC address entries are deleted.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the upper limit of dynamic MAC addresses learned from an interface.

max-dynamic-mac-count *count*

No upper limit of learned MAC addresses is configured for an interface by default.

(5) (Optional) Configure a forwarding rule to be used after the number of dynamic MAC addresses learned from an interface reaches the upper limit.

max-dynamic-mac-count exceed-action { **forward** | **discard** }

By default, after the number of MAC addresses learned from an interface reaches the upper limit, the device continues forwarding packets whose source MAC address is not learned.

1.8 Configuring Aging Time of Dynamic MAC Address Entries

1. Overview

The device deletes useless dynamic MAC address entries based on the aging time to save entry resources on the device. An overly long aging time may lead to untimely deletion of useless entries, whereas an overly short aging time may lead to deletion of some valid entries and repeated learning of MAC addresses by the device, which increases the packet broadcast frequency. Therefore, you are advised to configure a proper aging time of dynamic MAC address entries as required to save device resources without affecting network stability.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the aging time of dynamic MAC addresses.

mac-address-table aging-time *time*

The aging time of dynamic MAC addresses is 300s by default.

1.9 Enabling MAC Address Flapping Detection and Protection

1.9.1 Overview

If a MAC address is learned from different interfaces in the same VLAN, MAC address flapping occurs. If MAC address flapping occurs frequently between two specific interfaces, a network loop is formed. In this case, packets with the same source MAC address are received from different interfaces, and the MAC address entry is updated frequently. By enabling MAC address flapping detection, you can effectively monitor MAC address flapping events on the L2 network. Each time a MAC address flapping event occurs, the device reports a log alarm message. You can configure the MAC address flapping protection policy on the interfaces. When the device detects that MAC address flapping occurs between two interfaces with different priorities, the device reports an alarm message and disables the lower-priority interface.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure MAC address flapping detection.

mac-address-table flapping-logging

MAC address flapping detection is disabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) (Optional) Configure a MAC address flapping protection policy.

mac-address-table flapping action { **error-down** | **priority** *priority* }

No MAC address flapping protection policy is configured by default.

The MAC address flapping protection policy is available only for an interface with MAC address flapping detection enabled.

1.10 Configuring Reporting Interval of MAC Address Table Usage Alarms and MAC Address Table Usage Threshold

1.10.1 Overview

When the usage of a MAC address table of a device exceeds the upper or lower limit, the device reports an alarm message. With this function, you can adjust the reporting interval of MAC address table usage alarms and MAC address table usage threshold (in percentage).

When the usage of a MAC address table is higher than the upper limit, the device reports an alarm message at the specified interval. After the usage drops below the upper limit, the device reports a restoration message and stops reporting the alarm message. When the usage of a MAC address table is lower than the lower limit, the device reports an alarm message at the specified interval. After the usage rises above the lower limit, the device reports a restoration message and stops reporting the alarm message.

1.10.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a reporting interval of the MAC address table usage alarms.

mac-address-table warning-interval *interval*

The reporting interval of the MAC address table usage alarms is 3600s by default.

If you set the interval to 0s, MAC address table usage alarm reporting is disabled.

(4) Configure the upper and lower limits of the MAC address table usage.

mac-address-table warning-threshold upper-limit *upper-limit-threshold* **lower-limit** *lower-limit-threshold*

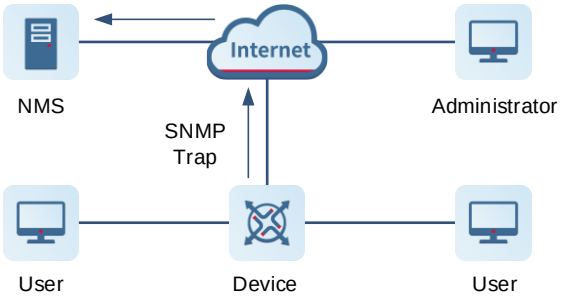
By default, the upper and lower limits for reporting MAC address table usage alarms are 80% and 70%, respectively.

1.11 Configuring the Function of MAC Address Entry Change Notification

1.11.1 Overview

After the function of MAC address entry change notification is configured on a device, the device generates a notification message for a MAC address entry change when the device learns a new MAC address or has aged a learned MAC address. In addition, the device sends the notification message in SNMP Trap mode to a specified Network Management Station (NMS). This function helps the network administrator monitor user change of network devices.

Figure 1-3 Application Scenario of the Function of MAC Address Entry Change Notification



As shown in Figure 1-3, when the device generates a notification for an added MAC address, a new user identified by the MAC address starts to use the network. When the device generates a notification for a deleted MAC address, the corresponding user does not send packets in the address aging time. In this case, it is considered that the user stops using the network. When the device is accessed by a large number of users, the device may generate a large number of MAC address entry change notifications in a short time, and the traffic increases.

To reduce traffic, you can configure an interval for sending MAC address entry change notifications. When the configured interval arrives, the system sends all notifications in a period of time at a time. This helps reduce the network traffic. Each notification message contains information about several MAC address changes.

A generated notification is stored in a history table for MAC address entry change notifications. The administrator may know recent MAC address changes by checking the history table even without NMS.

1.11.2 Restrictions and Guidelines

A MAC address entry change notification is generated only for a dynamic MAC address entry.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an NMS host address for receiving MAC address entry change notifications.

snmp-server host { *ipv4-address* | **ipv6** *ipv6-address* } **traps** [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }] *community-string*

No NMS host address is configured for receiving MAC address entry change notifications by default.

(4) Enable sending of MAC address entry change notifications in Trap messages.

snmp-server enable traps

Sending Trap messages to the NMS host is forbidden by default.

(5) Enable the function of MAC address entry change notification in global configuration mode.

mac-address-table notification

The function of MAC address entry change notification is disabled in global configuration mode by default.

(6) (Optional) Configure an interval for sending MAC address entry change notifications.

mac-address-table notification interval *interval*

The device sends MAC address entry change notifications at an interval of 1s by default.

(7) (Optional) Configure the size of a history table for MAC address entry change notifications.

mac-address-table notification history-size *size*

The size of the history table for MAC address entry change notifications is 50 by default.

(8) Enter the interface configuration mode.

interface *interface-type interface-number*

(9) Enable the function of MAC address entry change notification for an interface.

snmp trap mac-notification { **added** | **removed** }

The function of MAC address entry change notification is disabled for an interface by default.

1.12 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

You can run the **clear** commands to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear mac-address-table dynamic [**address** *mac-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]	Clears the dynamic MAC address entries.
clear mac-address-table flapping record	Clears the MAC address flapping records.

show mac-address-table { **dynamic** | **static** | **filter** } [**address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-id*]	Displays the MAC address table.
show mac-address-table { **evpn** | **mlag** }	Displays the EVPN or MLAG address table.
show mac-address-table address *mac-address* [**vsi** *vsi-id*] [**vni** *vni-id*]	Displays the specific EVPN or MAC address table.
show mac-address-table [**vsi** *vsi-id*] [**vni** *vni-id*]	Displays the specific VNI or VSI address table.
show mac-address-table all	Displays all types of addresses.
show mac-address-table aging-time	Displays the aging time for dynamic MAC addresses.
show mac-address-table max-dynamic-mac-count	Displays the maximum number of dynamic MAC addresses.
show mac-address-table notification [**interface** [*interface-type interface-number*] **| history**]	Displays the configurations and history table for MAC address entry change notifications.
show mac-address-table flapping record	Displays the dynamic MAC address flapping records.

1.13 Configuration Examples

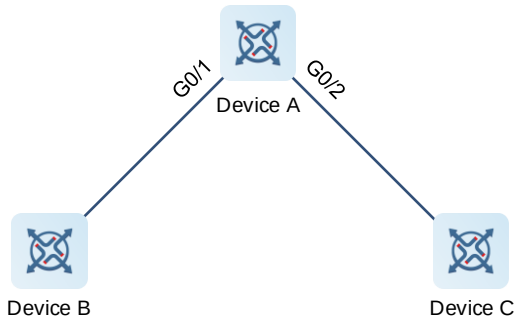
1.13.1 Configuring MAC Address Flapping Detection

1. Requirements

As shown in Figure 1-4, an L2 loop may occur between Device B and Device C due to misoperation. After you enable MAC address flapping detection and configure a protection policy, the device can report alarms upon loops, and disable the faulty interface based on the protection policy.

2. Topology

Figure 1-4 MAC Address Flapping Detection



3. Notes

- Enable MAC address flapping detection on Device A.

- Configure a MAC address flapping protection policy on the interfaces of Device A.
- Set the priority of GigabitEthernet 0/1 to be higher than that of GigabitEthernet 0/2 on Device A.

4. Procedure

Enable MAC address flapping detection.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# mac-address-table flapping-logging
```

Configure a protection policy to disable GigabitEthernet 0/1 upon MAC address flapping and set the priority of this interface to **5**.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config)# (config-if-GigabitEthernet 0/1)# mac-address-table flapping action error-down
DeviceA(config)# (config-if-GigabitEthernet 0/1)# mac-address-table flapping action priority 5
DeviceA(config)# (config-if-GigabitEthernet 0/1)# exit
```

Configure a protection policy to disable GigabitEthernet 0/2 upon MAC address flapping and set the priority of this interface to **1**.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config)# (config-if-GigabitEthernet 0/2)# mac-address-table flapping action error-down
DeviceA(config)# (config-if-GigabitEthernet 0/2)# mac-address-table flapping action priority 1
```

5. Verification

After the preceding configuration, the device generates an alarm message when MAC address flapping from GigabitEthernet 0/1 to GigabitEthernet 0/2 occurs. Run the **show mac-address-table flapping record** command to display the dynamic MAC address flapping records.

View the records on Device A after MAC address flapping is detected.

```
DeviceA# show mac-address-table flapping record
 Mac address flapping detect status      : on
 Mac address flapping detect interval    : 1s
 Mac address flapping syslog supress time : 1800s
 Mac address flapping record max count   : 300
 Mac address flapping record total count  : 2

 Move-Time          VLAN  MAC-Address    Original-Port   Move-Ports   Status
 ------------------- ----- -------------- --------------- ------------ --------
 2020.11.14 12:10:46 1     0001.1111.1111 ge0/1          ge0/2        Normal
 2020.11.14 12:10:58 1     0001.1111.1111 ge0/2          ge0/1        ERR-DOWN
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
```

```
!
mac-address-table flapping-logging
!
!
interface gigabitEthernet 0/1
mac-address-table flapping action error-down
mac-address-table flapping action priority 5
!
!
interface gigabitEthernet 0/2
mac-address-table flapping action error-down
mac-address-table flapping action priority 1
!
```

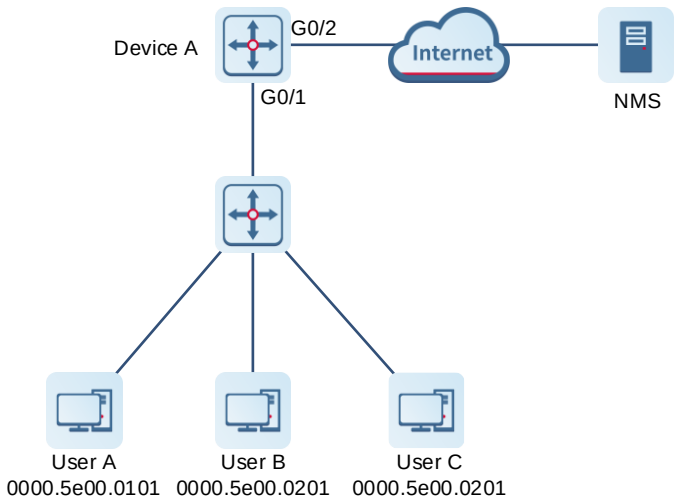
1.13.2 Configuring the Function of MAC Address Change Notification

1. Requirements

As shown in Figure 1-5, Device A is connected to devices of User A, User B, and User C, so that Device A records new MAC address entries learned from GigabitEthernet 0/1 and aged MAC address entries, sends MAC address entry change notifications to the specified NMS in SNMP Trap messages, and does not generate massive MAC address change information in a short time to prevent overusing network resources.

2. Topology

Figure 1-5 Function of MAC Address Entry Change Notification



3. Notes

- Enable the function of MAC address entry change notification in global configuration mode on Device A and configure an interval for sending MAC address Trap messages.
- Enable the function of MAC address entry change notification on GigabitEthernet 0/1 of Device A.
- Specify an SNMP host address and enable Trap notification of MAC address events.

- Ensure that the route between Device A and the NMS is reachable.

4. Procedure

Enable the function of MAC address entry change notification in global configuration mode on Device A and set the interval for sending MAC address Trap messages to 300s.

```
DeviceA# configure terminal
DeviceA(config)# mac-address-table notification
DeviceA(config)# mac-address-table notification interval 300
```

Enable the function of MAC address entry change notification on GigabitEthernet 0/1 and enable the function of sending Trap messages upon MAC address addition or deletion.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added
DeviceA(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed
```

Set the SNMP host address to 192.168.1.1, SNMP version to SNMP v1 and community string to **123** to actively send MAC address Trap messages.

```
DeviceA(config-if-GigabitEthernet 0/2)# exit
DeviceA(config)# snmp-server host 192.168.1.10 traps version 2c 123 mac-notification
```

Enable Trap notification of MAC address events.

```
DeviceA(config)# snmp-server enable traps
```

5. Verification

After the preceding configuration, run the **show mac-address-table notification** command to display the configuration status of the function of MAC address entry change notification in global configuration mode. Run the **show mac-address-table notification history** command to display the history table for MAC address entry change notifications.

Display the configuration status of the function of MAC address entry change notification in global configuration mode.

```
DeviceA# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
```

Display the history table for MAC address entry change notifications after the MAC address changes.

```
DeviceA# show mac-address-table notification history
History Index : 0
Entry Timestamp: 221683
MAC Changed Message :
Operation:ADD Vlan:1 MAC Addr: 0000.5e00.0201 GigabitEthernet 0/1
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
```

```
mac-address-table notification
mac-address-table notification interval 300
!
!
interface GigabitEthernet 0/1
 snmp trap mac-notification added
 snmp trap mac-notification removed
!
!
snmp-server host 192.168.1.10 traps version 2c 7 $10$135$2c+O$ mac-notification
snmp-server enable traps
!
```

Contents

1 Configuring MAC Loopback 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Configuring Basic Features 1

1.2.1 Overview 1

1.2.2 Procedure 1

1.3 Monitoring 2

1 Configuring MAC Loopback

1.1 Introduction

1.1.1 Overview

Media Access Control (MAC) loopback refers to a case in which packets sent from a local end are transferred internally in the system and returned to the local end for interface self-loop.

MAC loopback can be used to determine whether an Ethernet interface is faulty. For an interface with MAC loopback enabled, if the interface runs normally, the physical status of the interface is always up even without network cable connection; and if the interface runs abnormally, the physical status of the interface is down.

MAC loopback can be applied to multi-port mirroring scenarios. One-to-many mirroring can be implemented by configuring an interface as a MAC loopback interface, and adding the mirroring destination port and expected outbound mirroring port to a remote VLAN.

1.1.2 Principles

After a MAC loopback interface is configured on a device, the chip of the device sends test packets and then receives these packets through the loopback created internally. By this, the loopback test of the interface is completed.

Caution

With MAC loopback enabled on an interface, data forwarding on this interface is abnormal. After the test, disable MAC loopback.

1.2 Configuring Basic Features

1.2.1 Overview

This section describes how to enable MAC loopback on an interface for interface self-loop.

1.2.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an interface as a loopback interface, and enable MAC loopback on the interface.

mac-loopback

MAC loopback is disabled for an interface by default.

(5) Disable MAC loopback after the test.

no mac-loopback

MAC loopback is disabled for an interface by default.

1.3 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

Table 1-1 MAC Loopback Monitoring

Command	Purpose
show mac-loopback	Displays the loopback interface configuration status of the current device.

Contents

1 Configuring VLAN....1
1.1 Introduction....1
1.1.1 Overview....1
1.1.2 Background and Functions....1
1.1.3 Frame Format....2
1.1.4 Port Types and Link Types....3
1.1.5 Principles....5
1.1.6 VLAN Assignment Methods....13
1.1.7 Protocols and Standards....14
1.2 Restrictions and Guidelines....14
1.3 Configuration Task Summary....14
1.4 Configuring VLAN....15
1.4.1 Overview....15
1.4.2 Restrictions and Guidelines....15
1.4.3 Configuration Tasks....15
1.4.4 Creating and Configuring VLAN....15
1.4.5 Configuring VLAN Name....16
1.4.6 Configuring L3 SVI of VLAN....16
1.5 Configuring Access Port....17
1.5.1 Overview....17
1.5.2 Restrictions and Guidelines....17
1.5.3 Prerequisites....17

1.5.4 Procedure....17

1.6 Configuring Trunk Port....18

1.6.1 Overview....18

1.6.2 Restrictions and Guidelines....18

1.6.3 Prerequisites....19

1.6.4 Procedure....19

1.7 Configuring Uplink Port....20

1.7.1 Overview....20

1.7.2 Restrictions and Guidelines....20

1.7.3 Prerequisites....20

1.7.4 Procedure....20

1.8 Configuring Hybrid Port....21

1.8.1 Overview....21

1.8.2 Restrictions and Guidelines....21

1.8.3 Prerequisites....22

1.8.4 Procedure....22

1.9 Monitoring....22

1.10 Configuration Examples....23

1.10.1 Configuring L2 Isolation and L3 Interconnection of VLAN....23

1 Configuring VLAN

1.1 Introduction

1.1.1 Overview

A virtual local area network (VLAN) is a logical network created by dividing a physical network. Every VLAN has an independent broadcast domain, and different VLANs are isolated on layer 2 (L2). Devices on different VLANs can implement communication through layer 3 (L3) devices or L3 interfaces.

1.1.2 Background and Functions

1. Background

The earliest local area network (LAN) adopts a bus structure, and STAs on the bus belong to the same contention domain. Bridges and L2 switches can isolate STAs onto different ports and control packet forwarding to isolate the contention domain. All ports of L2 switches belong to the same broadcast domain. When a switch receives a frame with an unknown destination address, the switch broadcasts this frame to all ports in the broadcast domain other than the source port. After receiving a reply from a port that matches the destination address, the switch learns the new MAC address based on the source address in the reply packet. This is the basic working mode of the switch.

If the network scale is enlarged, the increasing broadcast packets waste bandwidth. In addition, each STA in the broadcast domain can receive broadcast packets in the entire LAN. If users capture these packets using a packet capture tool, the content in the packets may be intercepted, which affects information security.

Routers communicate based on L3 IP addresses, and different subnets belong to different broadcast domains. This dampens the forwarding of broadcast packets. However, high forwarding performance of routers depends on central processing units (CPUs), and requires a high cost. Therefore, routers are usually used as egresses between LANs and wide area networks (WANs). Based on the concept of router subnet, a VLAN is developed.

2. Functions

You can divide a physical LAN into multiple VLANs by using different division methods so as to isolate broadcast domains, which saves bandwidth and enhances LAN security.

3. Features

- L2 isolation

  A VLAN shares the same attributes with a common physical LAN except the restriction on physical location. Every VLAN has an independent broadcast domain. If no switch virtual interface (SVI) is configured for VLANs, the VLANs are mutually isolated on L2. Users in different VLANs cannot communicate with each other. L2 unicast, broadcast and multicast frames are forwarded and transmitted in the same VLAN without entering other VLANs.

- L3 interconnection

  In an L3 switch, each VLAN corresponds to an SVI and the SVI functions as a VLAN gateway to implement L3 communication between VLANs.

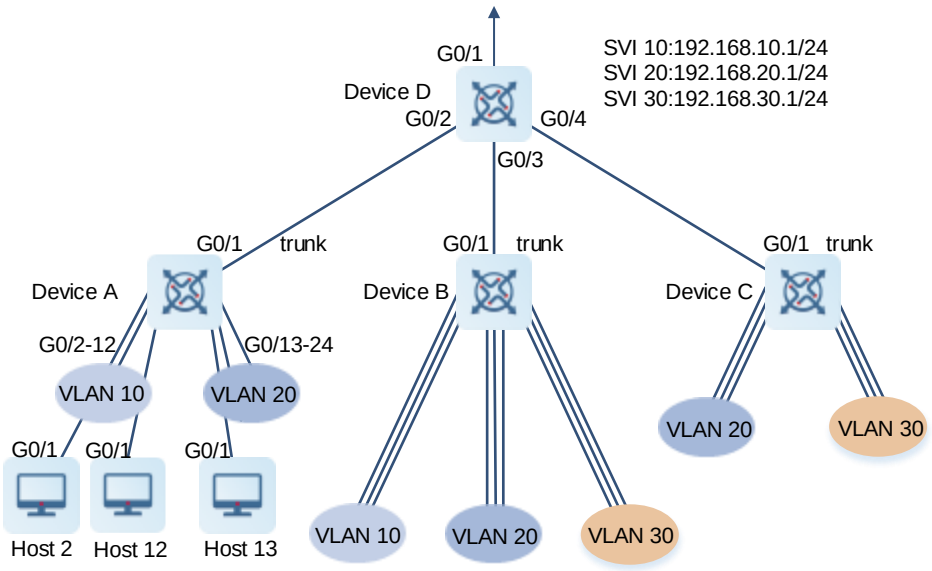
4. Application

As shown in Figure 1-1, VLANs are created on Device A, Device B, and Device C, and the LAN is divided into VLAN10, VLAN20, and VLAN30. The VLANs are mutually isolated on L2.

A port is defined as a VLAN member. All STAs connected to the port are a part of the VLAN. To change the VLAN of a user, modify the VLAN configuration of the port without adjusting the physical position of the user.

On the core device Device D, configure three VLANs, configure the ports to be connected to Device A, Device B, and Device C as trunk ports, and specify an allowed VLAN list. Three SVIs are configured as gateway interfaces of IP subnets corresponding to the three VLANs, and IP addresses are configured accordingly. The three VLANs enable subnet interconnection based on the IP forwarding capability of the L3 core device.

Figure 1-1 Typical Scenario

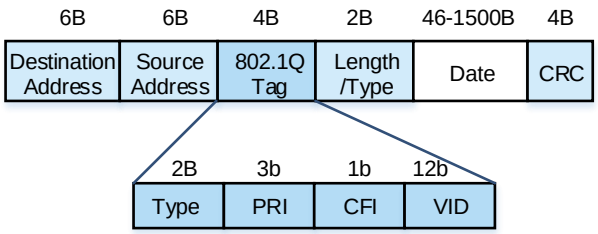


1.1.3 Frame Format

Based on IEEE 802.1Q, a 4-byte 802.1Q tag is inserted between the source MAC address field and protocol type field of an Ethernet frame, as shown in Figure 1-2. The VLAN ID (VID) field in the tag is used to represent the VLAN where the frame comes from. Not all devices identify tagged 802.1Q frames. Therefore, Ethernet frames can be tagged or untagged in the VLAN.

- Type: two bytes. The value **0X8100** indicates 802.1Q frames. Devices not supporting 802.1Q discard these frames upon receiving them.
- PRI: three bits. It indicates the L2 priority and corresponds to the Class of Service (CoS) priority of the Quality of Service (QoS). The value range is from 0 to 7. A larger value indicates a higher priority.
- CFI: one bit. It differentiates among Ethernet frames, Fiber Distributed Data Interface (FDDI) frames, and token ring network frames. The value **0** indicates Ethernet frames.
- VID: 12 bits. It indicates the ID of a VLAN to which packets belong. The value range is from 1 to 4094, and the value **0** and **4095** are reserved.

Figure 1-2 802.1Q Frame Format



This product complies with IEEE 802.1Q and supports a maximum of 4094 VLANs. The value range of the VLAN ID is from 1 to 4094. VLAN 1 is a default VLAN that does not need to be created and cannot be deleted. Other VLANs can be created and deleted. When you create a VLAN, the system returns a VLAN creation failure message if hardware resources are insufficient.

1.1.4 Port Types and Link Types

Ports can be classified into L2 interfaces and L3 interfaces. Only L2 interfaces can be added to VLANs. Table 1-1 lists different types of VLAN ports. You can configure the type of a VLAN port to determine the types of frames supported by the port, the number of VLANs supported by the port, and whether packets to be forwarded by the port carry the tag field.

Table 1-1 Port Types

Port Type	Function
Access port	An access port must belong to one VLAN. Therefore, only frames from this VLAN can pass the port. This VLAN is referred to as access VLAN, which is a native VLAN and also an allowed VLAN. All access ports belong to VLAN 1 by default. The frames sent from the access port do not carry tags. When the access port receives an untagged frame from a peer device, the local device determines that the frame comes from the access VLAN and adds the access VLAN ID to the frame.
Trunk port	A trunk port has one native VLAN and multiple allowed VLANs. The native VLAN is VLAN 1 by default. The allowed VLANs are all VLANs (1 to 4094) of the local device. Therefore, the trunk port can forward frames of all VLANs. The frames forwarded by the trunk port from the native VLAN do not carry tags and the frames forwarded by the trunk port from allowed VLANs carry tags. Note that the trunk ports of a link must be configured with the same native VLAN.

Port Type	Function
Uplink port	An uplink port has one native VLAN and several allowed VLANs. The native VLAN is VLAN 1 by default. The allowed VLANs are all VLANs (1 to 4094) of the local device. Therefore, the uplink port can forward frames of all VLANs. Frames sent by the uplink port are tagged. In a QinQ scenario, frames sent by a Provider Edge (PE) device port connected to a public network must carry tags. Therefore, the port must be configured as an uplink port. A Customer Edge (CE) device port connected to the PE device can also be configured as an uplink port. For more information, see *QinQ*.
Hybrid port	A hybrid port has one native VLAN and multiple allowed VLANs. The allowed VLANs can be classified into tagged VLANs and untagged VLANs. The native VLAN is VLAN 1 by default. The allowed VLANs can be classified into untagged VLAN 1 and tagged VLANs 2 to 4094. Therefore, the hybrid port can forward frames of all VLANs. The frames forwarded by the hybrid port from a tagged VLAN carry tags, and the frames forwarded by the hybrid port from an untagged VLAN do not carry tags. The frames forwarded by the hybrid port from the native VLAN must not carry tags, because the native VLAN is an untagged VLAN. The MAC VLAN function applies to only untagged VLANs on the hybrid port. Therefore, the hybrid port can be used as an interface to connect to STAs in MAC VLAN scenarios. For more information, see *MAC VLAN*.
Dot1q-tunnel port	A Dot1q-tunnel port has one native VLAN and several allowed VLANs. The allowed VLANs can be classified into tagged VLANs and untagged VLANs. The native VLAN is VLAN 1 by default, and the allowed VLAN is untagged VLAN 1. If QinQ is enabled, the PE port connected to the user network encapsulates an outer VLAN tag to user packets and then transmits the packets in the operator network. The PE port must be configured as a Dot1q-tunnel port and the VLAN on the operator network must be configured as the native VLAN of the Dot1q-tunnel port. If packets are encapsulated using the basic QinQ method, the PE port uses the native VLAN ID as the VLAN ID of the outer VLAN tag. To ensure uplink and downlink packet transmission, the native VLAN must be added to the untagged VLAN allowed list of the Dot1q-tunnel port. For more information, see *QinQ*.

VLAN links include access links and trunk links.

- An access link connects STAs to a switch port. Generally, the STA hardware cannot identify frames that carry VLAN tags. Therefore, the frames transmitted between the STAs and access ports are untagged frames. The access port and hybrid port can be connected by the access link. Some STAs can identify frames that carry VLAN tags. The actual product prevails.
- A trunk link can bear data of different VLANs. You must ensure that the devices connected by the trunk link can identify the VLAN of frames transmitted on the trunk link. The trunk port, uplink port, and Dot1q-tunnel port can be connected by the trunk link only. The hybrid port can be connected by both the trunk link and the access link. To transmit untagged frames from the native VLAN on the trunk link, ensure that the native

VLAN configuration on the peer device is consistent with that on the local device.

1.1.5 Principles

1. Frame Processing Rules

- Frame receiving rule

  When detecting an incoming untagged frame, if the port regards that the frame comes from the native VLAN, the port receives the packet, and identifies the frame as one from the native VLAN.

  When detecting a tagged frame, the port receives the packet if the port allows the VLAN identified by the tag. Otherwise, the port discards the packet.

- Frame forwarding rule

  An L2 switch can forward packets to only ports that match allowed VLANs (other than the source port).

  An L3 switch can determine an egress VLAN by querying the routing table in software and forward packets to a port that allows the egress VLAN.

- Frame sending rule

  After packets are forwarded in the switch, the switch determines whether to add tags to the packets based on the VLAN type (tagged VLAN or untagged VLAN).

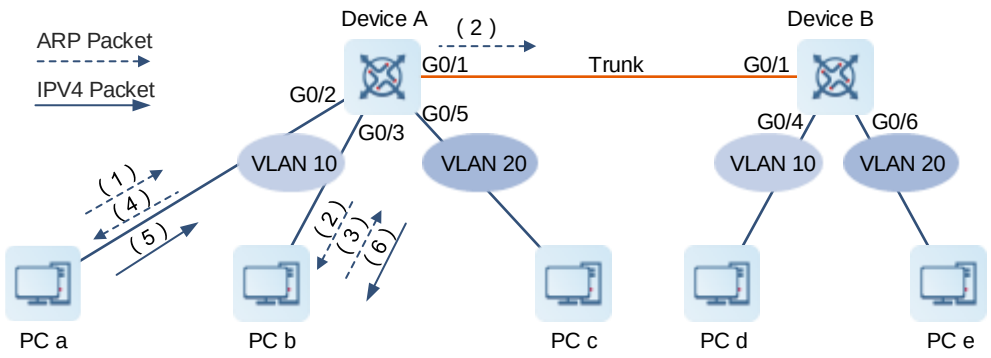
Table 1-2 Port Examples

Port	Mode	Native VLAN	Allowed VLAN List	Allowed VLAN Type
Gi 0/0	Access	10	10	10 (untagged)
Gi 0/1	Trunk	10	10, 20, 30	10 (untagged), 20 (tagged), and 30 (tagged)
Gi 0/2	Hybrid	20	10, 20, 30	20 (untagged), 10 (tagged), and 30 (tagged)
Gi 0/3	Uplink	30	20, 30	30 (tagged) and 20 (tagged)

As described in Table 1-2, when GigabitEthernet 0/0 receives an untagged frame or a frame with a VLAN 10 tag, it forwards the frame to GigabitEthernet 0/1 and GigabitEthernet 0/2 that allow VLAN 10. The VLAN 10 frame sent to GigabitEthernet 0/1 is untagged, and the VLAN 10 frame sent to GigabitEthernet 0/2 is tagged. When GigabitEthernet 0/3 receives a frame with a VLAN 30 tag, it forwards the frame to GigabitEthernet 0/1 and GigabitEthernet 0/2 that allow VLAN 30. The VLAN 30 frame sent to GigabitEthernet 0/1 is tagged, and the VLAN 30 frame sent to GigabitEthernet 0/2 is untagged.

2. Intra-VLAN Communication Within One Device

Figure 1-3 Example of Intra-VLAN Communication Within One Device



As shown in Figure 1-3, the mappings between ports and VLANs on Device A are as follows:

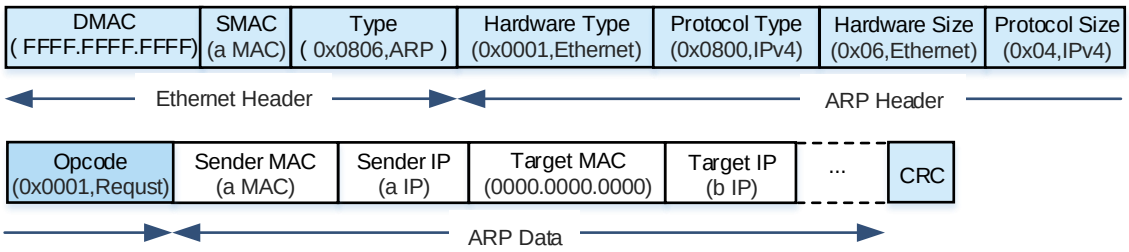
```
VLAN     Name       Status     Ports
10       VLAN10     STATIC     Gi0/1, Gi0/2, Gi0/3
20       VLAN20     STATIC     Gi0/1, Gi0/5
```

PC a and PC b belong to VLAN 10. Their communication procedure is as follows:

(1) To communicate with PC b (1.1.10.3/24), PC a (1.1.10.2/24) first determines that it is in the same subnet as PC b and queries the Address Resolution Protocol (ARP) table for the MAC address corresponding to the IP address of PC b. If PC a finds the MAC address of PC b, go to step (5) . If PC a does not find the MAC address of PC b, PC a sends an ARP request packet encapsulated in an Ethernet broadcast frame to PC b, as shown in Figure 1-4.

```
Protocol      Address              Age(min)    Hardware        Type
Internet      1.1.10.3              0                         arpa
```

Figure 1-4 ARP Request Packet Sent by PC a for Requesting MAC Address of PC b



Upon receiving the ARP request packet of PC a from GigabitEthernet 0/2 (as shown in Figure 1-4), if Device A finds that the packet is untagged, it determines that the packet comes from VLAN 10 and receives the packet. Device A learns the source IP address in the packet, and enters the mapping among the IP address, MAC address, port, and VLAN of PC a into the ARP table.

```
Protocol     Address     Age(min)    Hardware        Type    Interface
Internet     1.1.10.2     0          a MAC           arpa    Gi0/2
```

Device A enters the mapping among the VLAN, MAC address, and port of PC a into the dynamic MAC address table.

```
Vlan        MAC Address      Type         Interface
10          a MAC           Dynamic      Gi0/2
```

(2) Device A searches for the port that allows VLAN 10, and broadcasts the ARP request to GigabitEthernet 0/1 and GigabitEthernet 0/3.

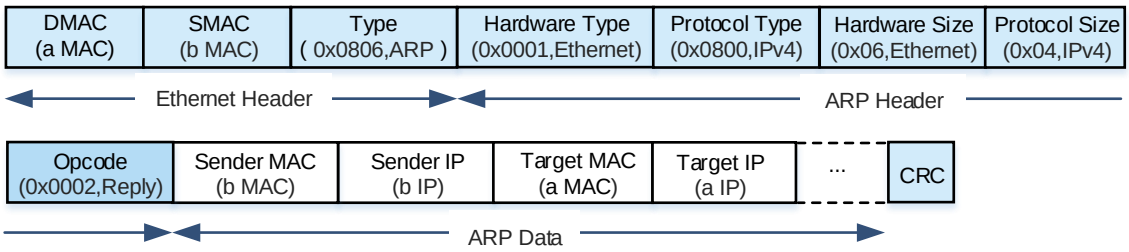
```
VLAN     Name      Status     Ports
10       VLAN10    STATIC     Gi0/1, Gi0/2, Gi0/3
20       VLAN20    STATIC     Gi0/1, Gi0/5
```

PC b receives the ARP request (as shown in Figure 1-4) of PC a from GigabitEthernet 0/3, learns the mapping between the IP address and MAC address of PC a, and enters the mapping into the ARP table.

```
Protocol  Address     Age(min)    Hardware       Type
Internet  1.1.10.2    0          a MAC          arpa
```

(3) If PC b finds that the destination IP address in the ARP request matches its own IP address, it sends an ARP reply to PC a in unicast mode (as shown in Figure 1-5).

Figure 1-5 ARP Reply Packet Sent by PC b to PC a



Upon receiving the ARP reply (as shown in Figure 1-5) of PC b from GigabitEthernet 0/3, Device A learns the source IP address and enters the mapping among the IP address, MAC address, port, and VLAN of PC b into the ARP table.

```
Protocol  Address     Age(min)    Hardware       Type   Interface
Internet  1.1.10.2     1          a MAC          arpa   Gi0/2
Internet  1.1.10.3     0          b MAC          arpa   Gi0/3
```

Device A enters the mapping among the VLAN, MAC address, and port of PC b into the dynamic MAC address table.

```
Vlan        MAC Address      Type         Interface
10          a MAC           Dynamic      Gi0/2
10          b MAC           Dynamic      Gi0/3
```

(4) Device A queries the MAC address table, hits the MAC address of PC a, and forwards the ARP reply of PC b to GigabitEthernet 0/2.

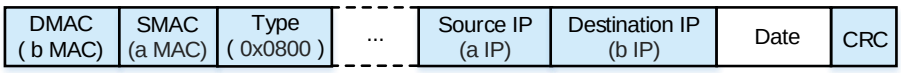
PC a receives the ARP reply (as shown in Figure 1-5) of PC b from GigabitEthernet 0/2, learns the mapping between the IP address and MAC address of PC b, and enters the mapping into the ARP table.

(5) PC a finds the MAC address of PC b in the ARP table, generates a packet with the MAC address of PC b as the destination MAC address and the MAC address of PC a as the source MAC address, and sends the packet to PC b (as shown in Figure 1-6).

```
Protocol     Address            Age(min)    Hardware      Type
```

```
Internet      1.1.10.3            0          b MAC         arpa
```

Figure 1-6 IPv4 Packet Sent from PC a to PC b



(6) Upon receiving the packet from PC a, Device A refreshes the MAC address table based on the source IP address of PC a, queries the MAC address table to hit the destination MAC address of PC b, and forwards the packet to GigabitEthernet 0/3 (as shown in Figure 1-6).

3. Inter-VLAN Communication

Devices from different VLANs may need to communicate with each other. The VLAN broadcast domains are isolated on L2. Therefore, the devices from different VLANs can communicate with each other by using an L3 device, for example, by using a routing device for relay. This method requires router ports. A routing module can be added to the L2 switch to form an L3 switch.

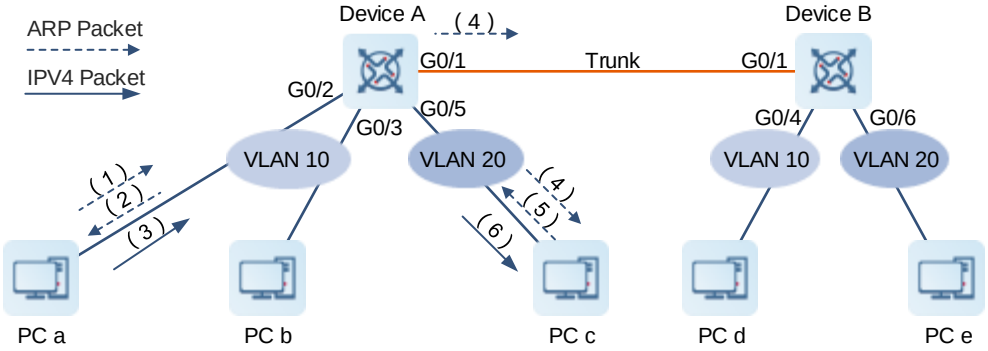
On the L3 switch, one VLAN corresponds to one SVI. The L3 switch takes the SVI as an independent interface, creates an ARP entry for the interface, and records the mapping between the IP address and MAC address of the SVI.

A STA in each VLAN uses the IP address of an SVI corresponding to this VLAN as the default gateway. When the STA in the VLAN tries to communicate with an STA in another VLAN, the STA queries the MAC address of the gateway, and then forwards a packet to the gateway.

When the L3 switch receives the packet whose MAC address matches the SVI, the switch enables L3 forwarding. If the L3 switch does not know the MAC address of the destination host, the L3 switch queries the routing table in the software, determines the egress VLAN of the destination host, and sends an ARP request in the egress VLAN. Upon obtaining an ARP reply from the destination host, the L3 switch learns the IP address, MAC address, port, and VLAN of the destination host, updates the L3 routing table, replaces the source MAC address in the packet with the MAC address of the gateway and the destination MAC address with the MAC address of the destination host, and forwards the packet to the destination host. Later, when the L3 switch receives packets with the same destination MAC address, the L3 switch directly queries the L3 routing table, replaces the source and destination MAC addresses, and forwards the packets.

As shown in Figure 1-7, PC a belongs to VLAN 10 and PC c belongs to VLAN 20. Their communication is implemented across the VLANs.

Figure 1-7 Example of Inter-VLAN Communication



The mappings between ports and VLANs on Device A are as follows:

```
VLAN     Name       Status     Ports
10       VLAN10     STATIC     Gi0/1, Gi0/2, Gi0/3
20       VLAN20     STATIC     Gi0/1, Gi0/5
```

After an SVI is created, the switch generates the mappings of IP addresses to MAC addresses. The gateway MAC address is the MAC address of Device A.

```
VLAN     IP Address                Hardware Address
10       1.1.10.1                  g MAC
20       1.1.20.1                  g MAC
```

A direct route to L3 SVI is generated.

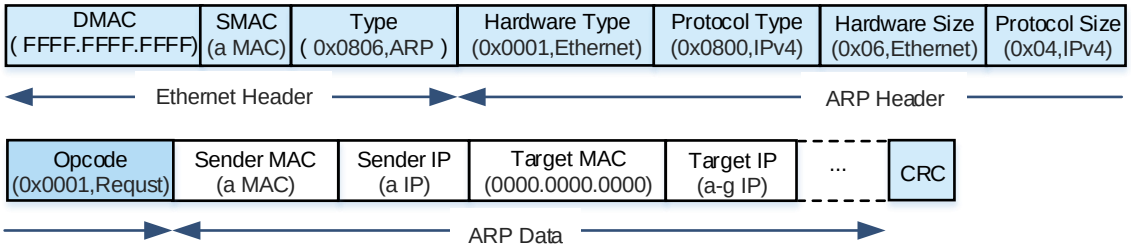
```
C       1.1.10.0/24 is directly connected, VLAN 10
C       1.1.20.0/24 is directly connected, VLAN 20
```

PC a and PC b belong to different VLANs. Their communication procedure is as follows:

(1) To communicate with PC c (1.1.20.5/24), PC a (1.1.10.2/24) first determines that they are in different subnets and queries the ARP table for the gateway MAC address corresponding to the gateway IP address (1.1.10.1/24) of PC a. If PC a finds the MAC address of the gateway, go to step (3) . If PC a does not find the MAC address of the gateway, it sends an ARP request packet encapsulated in an Ethernet broadcast frame to the gateway, as shown in Figure 1-8.

```
Protocol  Address      Age(min)    Hardware       Type
Internet  1.1.10.1      0                        arpa
```

Figure 1-8 ARP Request Packet Sent by PC a for Requesting MAC Address of the Gateway



Upon receiving the ARP request packet of PC a from GigabitEthernet 0/2 (as shown in Figure 1-8), if Device A finds that the packet is untagged, it determines that the packet comes from VLAN 10 and receives the packet.

Device A learns the source IP address in the packet, and enters the mapping among the IP address, MAC address, port, and VLAN of PC a into the ARP table.

```
Protocol  Address      Age(min)    Hardware       Type   Interface
Internet  1.1.10.2     0          a MAC          arpa   Gi0/2
```

Device A enters the mapping among the VLAN, MAC address, and port of PC a into the dynamic MAC address table.

```
Vlan        MAC Address       Type         Interface
10          a MAC            Dynamic      Gi0/2
```

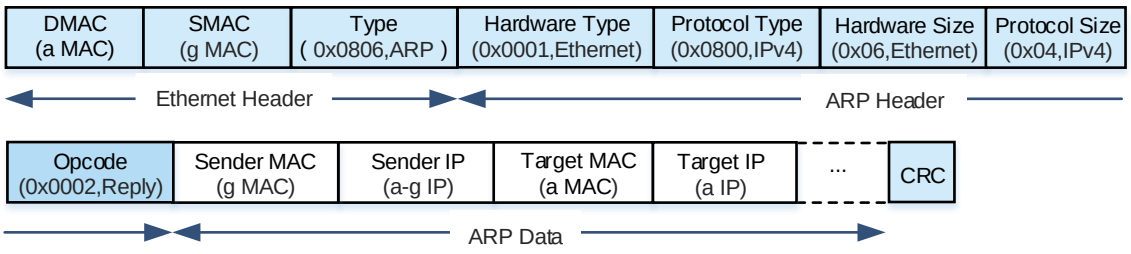
The preceding information constitutes the content of an L3 routing table. The routing table cannot be queried but its content is reflected in the ARP table and MAC address table.

```
VLAN     IP Address        Hardware         Interface
10       1.1.10.2         a MAC            Gi0/2
```

(2) If Device A finds that the packet is an ARP packet and the destination IP address in the packet is the IP address of the SVI corresponding to VLAN 10 of this device, it returns an ARP reply in unicast mode and

forwards the reply packet through GigabitEthernet 0/2. The reply packet (as shown in Figure 1-9) includes the IP address and MAC address of SVI 10.

Figure 1-9 ARP Reply Packet Sent by the Gateway to PC a

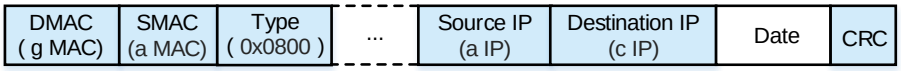


Upon receiving the ARP reply, PC a learns the MAC address corresponding to the IP address of the SVI 10 gateway and updates the ARP table of PC a.

(3) If PC a finds the MAC address of the gateway in the ARP table, it generates a packet with the gateway MAC address as the destination MAC address and the MAC address of PC a as the source MAC address, encapsulates the packet in an Ethernet frame (as shown in Figure 1-10), and forwards the packet to the gateway.

```
Protocol  Address      Age(min)    Hardware        Type
Internet  1.1.10.1     0           g MAC           arpa
```

Figure 1-10 IPv4 Packet Sent by PC a to PC c



(4) Upon receiving the packet of PC a from GigabitEthernet 0/2 (as shown in Figure 1-10), Device A refreshes the MAC address entry of PC a. If Device A finds that the packet is untagged, it determines that the packet comes from VLAN 10. The destination MAC address (gateway MAC address) is the MAC address of the local device. Therefore, the packet must be forwarded at L3. If Device A finds the MAC address of PC c corresponding to the IP address of PC c, go to step (6) . If Device A does not find this MAC address, it forwards the packet to the CPU for processing.

```
VLAN     IP Address       Hardware Address         Port
10       1.1.10.2         a MAC                    Gi0/2
         1.1.20.5
```

The CPU queries the routing table in the software, and finds that the packet matches a direct route to 1.1.20.0/24, with the egress VLAN being VLAN 20.

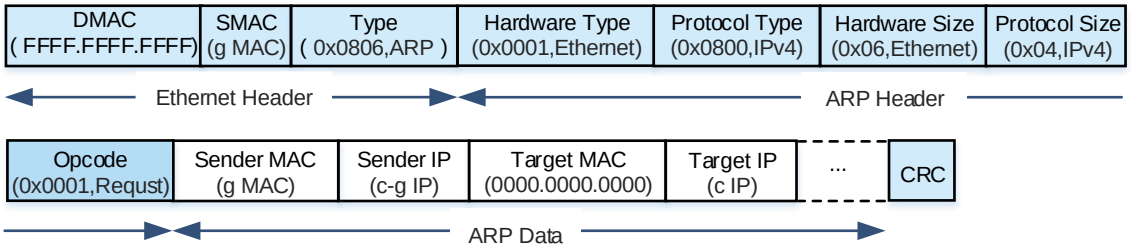
```
Connected    1.1.20.0/24 is directly connected, VLAN 20
```

The CPU continues to query the ARP table for the MAC address corresponding to the IP address of PC c, but the query fails.

```
Protocol  Address      Age(min)    Hardware     Type    Interface
Internet  1.1.20.5     0                        arpa
```

Device A broadcasts the ARP request (as shown in Figure 1-11) in the egress VLAN (VLAN 20) to request the MAC address of PC c. In this case, the IP address of the gateway is the address of the SVI in VLAN 20, that is, the gateway IP address (1.1.20.1/24) of PC c.

Figure 1-11 ARP Request Packet Sent by the Gateway for Requesting MAC Address of PC c



The ARP request is sent from GigabitEthernet 0/1 and GigabitEthernet 0/5 that allow VLAN 20.

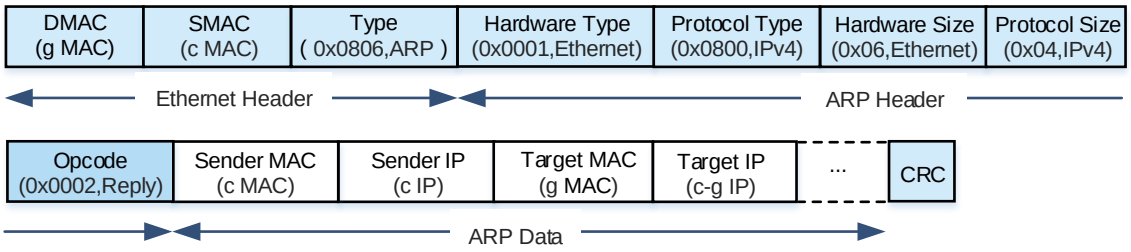
```
VLAN     Name       Status     Ports
10       VLAN10     STATIC     Gi0/1, Gi0/2, Gi0/3
20       VLAN20     STATIC     Gi0/1, Gi0/5
```

PC c receives the ARP request (as shown in Figure 1-11) of Device A from GigabitEthernet 0/5, learns the mapping between the gateway IP address and gateway MAC address in VLAN 20 on Device A, and enters the mapping into the ARP table.

```
Protocol  Address      Age(min)    Hardware       Type
Internet  1.1.20.1     0          g MAC          arpa
```

(5) If PC c finds that the destination IP address in the ARP request matches its own IP address, it sends an ARP reply packet in unicast mode (as shown in Figure 1-12).

Figure 1-12 ARP Reply Packet Sent by PC c to the Gateway



Upon receiving the ARP reply (as shown in Figure 1-12) of PC c, Device A learns the mapping among the IP address, MAC address, port, and VLAN of PC c, and enters the mapping into the ARP table.

```
Protocol  Address      Age(min)    Hardware       Type   Interface
Internet  1.1.10.2        1        a MAC         arpa   Gi0/2
Internet  1.1.20.5        0        c MAC         arpa   Gi0/5
```

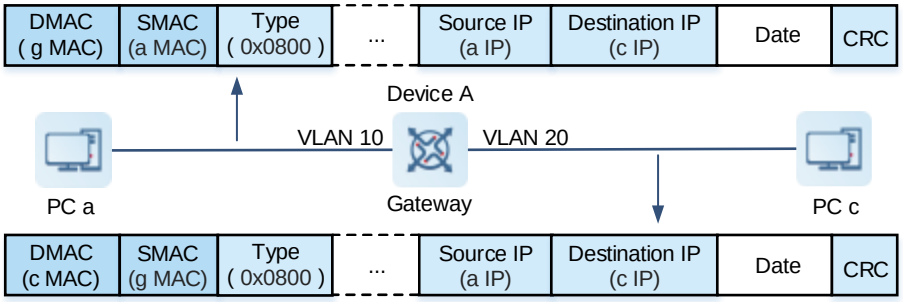
Device A enters the information about PC c into the dynamic MAC address table.

```
Vlan        MAC Address       Type         Interface
10          a MAC            Dynamic      Gi0/2
20          c MAC            Dynamic      Gi0/5
```

(6) If Device A finds the MAC address of PC c, it replaces the MAC address of PC a with the gateway MAC address and the gateway MAC address with the MAC address of PC c, and forwards the packet of PC a to PC c (as shown in Figure 1-13).

```
VLAN     IP Address       Hardware         Port
10       1.1.10.2         a MAC            Gi0/2
20       1.1.20.5         c MAC            Gi0/5
```

Figure 1-13 Packet Forwarded by the Gateway



PC c receives this packet (as shown in Figure 1-13) from GigabitEthernet 0/5, learns the mapping between the IP address of PC a and the gateway MAC address, and enters the mapping into the ARP table.

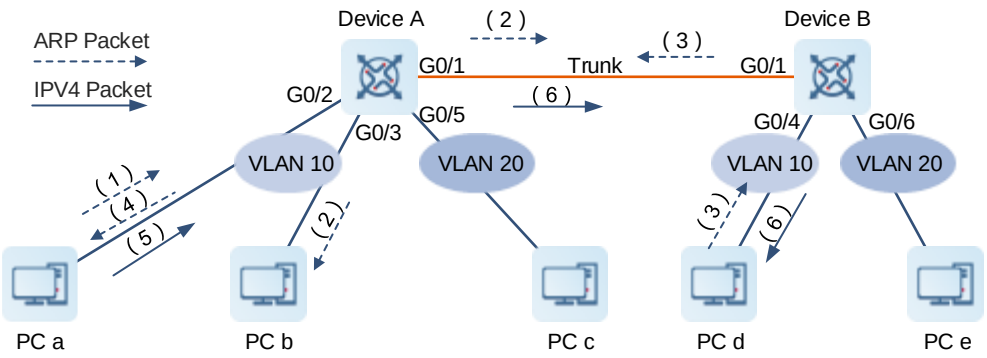
```
Protocol  Address      Age(min)    Hardware       Type
Internet  1.1.20.1       1         g MAC         arpa
Internet  1.1.10.2       0         g MAC         arpa
```

Later, when PC c sends the packet to PC a, it can query the gateway MAC address corresponding to the IP address of PC a, and encapsulate the packet for PC a by using the gateway MAC address as the destination MAC address.

4. Intra-VLAN Communication Across Devices

Ports on different devices can be assigned to the same VLAN. As shown in Figure 1-14, one port between two devices must allow packets from different VLANs to pass through, so that two PCs in the same VLAN can communicate across the devices. This interconnection port must be configured as a trunk port. PC a is connected to VLAN 10 through Device A, and PC d is connected to VLAN 10 through Device B. Device A and Device B are connected through the trunk port. The communication between PC a and PC d is intra-VLAN communication across devices.

Figure 1-14 Example of Intra-VLAN Communication Across Devices



The mappings between ports and VLANs on Device A are as follows:

```
Device A  VLAN    Name      Status    Ports
10              VLAN10    STATIC    Gi0/1, Gi0/2, Gi0/3
20              VLAN20    STATIC    Gi0/1, Gi0/5
```

The port configurations of Device A are as follows:

```
Device A Interface   Switchport   Mode    Access  Native   VLAN lists
Gi0/1              enabled     trunk           10      10,20
Gi0/2-Gi0/3         enabled     access   10             10
Gi0/5              enabled     access   20             20
```

The mappings between ports and VLANs on Device B are as follows:

```
Device B VLAN    Name      Status    Ports
10             VLAN10    STATIC    Gi0/1, Gi0/4
20             VLAN20    STATIC    Gi0/1, Gi0/6
```

The port configurations of Device B are as follows:

```
Device B Interface   Switchport   Mode    Access  Native   VLAN lists
Gi0/1              enabled    trunk           10      10,20
Gi0/4              enabled    access   10             10
Gi0/6              enabled    access   20             20
```

The procedure of intra-VLAN communication across devices is similar to the procedure of intra-VLAN communication within one device, except for the following:

- When Device A sends a packet through the trunk port GigabitEthernet 0/1, if the packet comes from the native VLAN (for example, the packet is sent by PC a to PC d in VLAN 10), the packet is untagged; or if the packet comes from an allowed VLAN (for example, the packet is sent by PC c to PC e in VLAN 20), the packet is tagged.
- When Device B receives the packet through the trunk port GigabitEthernet 0/1, if the packet is untagged (for example, the packet is sent by PC a to PC d in VLAN 10), Device B determines that the packet comes from the native VLAN (VLAN 10). If the native VLAN is also an allowed VLAN (VLAN 10 or VLAN 20), Device B allows the packet to pass through. If the native VLAN is not an allowed VLAN, Device B does not allow the packet to pass through. If the packet is tagged (for example, the packet is sent by PC c to PC e in VLAN 20), Device B checks whether the packet comes from an allowed VLAN (VLAN 10 or VLAN 20). If yes, Device B receives the packet. Otherwise, Device B discards the packet.

1.1.6 VLAN Assignment Methods

- Port-based assignment

Port-based VLAN assignment is the most basic VLAN assignment method. After the administrator configures a port with a Port Default VLAN ID (PVID), the port is assigned to a VLAN. The VLAN ID range is from 1 to 4094. In case of no VLAN assignment, all ports are assigned to VLAN 1 by default.

- Super VLAN

Super VLAN is also referred to as VLAN aggregation, which aggregates multiple VLANs into one IP address segment. Only one IP address is assigned to a super VLAN that contains multiple sub VLANs, and this saves address resources and facilitates network management. A VLAN accessible by an STA is subject only to an access port of the STA. That is, the STA is assigned to a VLAN based on the STA's access port. For more information, see *Super VLAN*.

- Private VLAN

Private VLAN is a technology that can divide an L2 broadcast domain of a VLAN into multiple sub domains, and each sub domain is composed of one private VLAN pair: primary VLAN and secondary VLAN. This technology can increase the number of users that can be supported by an operator network and reduce waste of IP address resources. A VLAN accessible by an STA is subject only to an access port of the STA. That is, the STA is assigned to a VLAN based on the STA's access port. For more information, see *Private VLAN*.

- MAC VLAN

MAC VLAN is a MAC address-based VLAN assignment method. When an STA is physically relocated, it can re-access the network from another device and there is no need to reconfigure a VLAN for the access port. If different STAs access the network from the same port, they can be assigned to different VLANs based on their MAC addresses. This method belongs to packet content-based VLAN assignment. Generally, this function is used with the 802.1x VLAN delivery function to ensure secure and flexible access of 802.1x STAs. For more information, see *MAC VLAN*.

- Voice VLAN

A voice VLAN is a VLAN dedicated for voice data streams of users. With this technology, data streams and voice streams are transmitted in the data VLAN and the voice VLAN, respectively, to prevent mutual interference between voice calls and service packets. This function identifies voice data and assigns the voice data to the voice VLAN. This method belongs to packet content-based VLAN assignment. For more information, see *Voice VLAN*.

- Protocol VLAN

Protocol VLAN is a VLAN assignment technology based on the protocol type or IP subnet in packets. The service types supported in a network are bound to VLANs to facilitate management and maintenance. This method belongs to packet content-based VLAN assignment. For more information, see *Protocol VLAN*.

1.1.7 Protocols and Standards

IEEE 802.1Q: IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks

1.2 Restrictions and Guidelines

Before you configure a port type or add the port to a VLAN, ensure that the port is an L2 interface. You can run the **switchport** command to configure an interface as an L2 interface. You can run the **no switchport** command to configure an interface as an L3 interface.

1.3 Configuration Task Summary

VLAN configuration includes the following tasks:

(1) Configuring VLAN

a Creating and Configuring VLAN

b (Optional) Configuring VLAN Name

c (Optional) Configuring L3 SVI of VLAN

(2) Configuring a port type and adding ports to a VLAN by performing at least one of the following configuration tasks:

- Configuring Access Port
- Configuring Trunk Port
- Configuring Uplink Port
- Configuring Hybrid Port

1.4 Configuring VLAN

1.4.1 Overview

This section describes how to create a VLAN, configure the VLAN, and enter the VLAN configuration mode.

1.4.2 Restrictions and Guidelines

In case of insufficient hardware resources, the system returns information on VLAN creation failure.

1.4.3 Configuration Tasks

VLAN configuration includes the following tasks:

(1) Creating and Configuring VLAN

(2) (Optional) Configuring VLAN Name

(3) (Optional) Configuring L3 SVI of VLAN

1.4.4 Creating and Configuring VLAN

1. Overview

You can create a VLAN or enter the VLAN configuration mode.

A VLAN is identified based on a VLAN ID, and the VLAN ID range is from 1 to 4094. VLAN 1 is created automatically and cannot be deleted. VLANs 2 to 4094 can be created, deleted, and edited.

2. Restrictions and Guidelines

- In case of insufficient hardware resources, the system returns information on VLAN creation failure.
- You can run the **no vlan** *vlan-id* command to delete a common VLAN. VLANs such as VLAN 1, VLANs with SVIs configured, and private VLANs cannot be deleted.
- To delete a VLAN with a created SVI, run the **no interface vlan** *vlan-id* command to delete the SVI and then the **no vlan** *vlan-id* command to delete the VLAN.

3. Prerequisites

Check VLAN and its VLAN status. If you enter a new VLAN ID, a corresponding VLAN is created. If you enter an existing VLAN ID, the system enters the configuration mode of the corresponding VLAN, and you can modify the VLAN settings.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a VLAN and enter the VLAN configuration mode.

vlan *vlan-id*

Only VLAN 1 exists by default.

1.4.5 Configuring VLAN Name

1. Overview

You can name a VLAN.

2. Restrictions and Guidelines

- You cannot rename a VLAN the same as the default name of another VLAN.
- To restore the VLAN name to a default value, run the **no name** command.

3. Prerequisites

The VLAN name must be unique.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VLAN configuration mode.

vlan *vlan-id*

(4) Configure a VLAN name.

name *vlan-name*

The name of a VLAN is its VLAN ID by default. For example, the name of VLAN 4 is VLAN0004.

1.4.6 Configuring L3 SVI of VLAN

1. Overview

You can create an L3 SVI of a VLAN and enter the SVI configuration mode. Configure an IP address for the SVI so that devices in the VLAN can communicate at L3.

2. Restrictions and Guidelines

- You cannot create SVIs for sub VLANs of a super VLAN or secondary VLANs of a private VLAN.
- To delete a VLAN with a created SVI, run the **no interface vlan** *vlan-id* command to delete the SVI and then the **no vlan** *vlan-id* command to delete the VLAN.

3. Prerequisites

Create a VLAN.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an SVI of a VLAN and enter the SVI configuration mode.

interface vlan *vlan-id*

No SVI is configured for a VLAN by default.

(4) (Optional) Configure an IP address and a mask for the VLAN gateway.

ip address *ip-address mask*

No IP address is configured for an SVI by default.

1.5 Configuring Access Port

1.5.1 Overview

You can define the type of an interface as L2 access port and add the interface to a VLAN.

1.5.2 Restrictions and Guidelines

- When you run the **switchport access vlan** *vlan-id* command to configure a VLAN for an access port, if you add the access port to an inexistent VLAN, the VLAN is automatically created. You can run the **no switchport access vlan** command to restore the VLAN for the access port to VLAN 1.
- The **add interface** { *interface-type interface-number* | **range** *interface-type interface-range* } command has the same execution effect as that of the **switchport access vlan** *vlan-id* command. You can run the **no add interface** { *interface-type interface-number* | **range** *interface-type interface-range* } command to restore the VLAN (other than VLAN 1) of a specified access port to VLAN 1.
- This command is available to access ports only. If you configure the command multiple times, the last command prevails.

1.5.3 Prerequisites

The interface to be configured must be an L2 interface. You can run the **show interface switchport** command to query the interface type. If the **Switchport** field corresponding to the interface is set to **enabled**, this interface is an L2 interface. Otherwise, this interface is an L3 interface. You should run the **switchport** command to configure the interface as an L2 interface and then set the default interface mode to **access**.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure one interface as an access port or a group of interfaces as access ports.

a Enter the configuration mode corresponding to the interface or the group of interfaces.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

b Configure the L2 interface as an access port.

switchport mode access

The L2 interface mode is **access** by default.

c Return to the global configuration mode.

exit

(4) (Optional) Add the interface or the group of interfaces to a VLAN. Select a method to configure the interface or the group of interfaces.

- Create a VLAN, and add the interface or the group of interfaces to the VLAN in VLAN configuration mode. Run the following commands in sequence:

  vlan *vlan-id*

  Only VLAN 1 exists by default.

  add interface { *interface-type interface-number* | **range** *interface-type interface-range* }

  An access port belongs to VLAN 1 by default.

- Add the interface or the group of interfaces to a VLAN (which can be automatically created) in interface configuration mode. Run the following commands in sequence:

  interface { *interface-type interface-number* | **range** *interface-type interface-range* }

  switchport access vlan *vlan-id*

  An access port belongs to VLAN 1 by default.

1.6 Configuring Trunk Port

1.6.1 Overview

A trunk link can transmit traffic of multiple VLANs. To enable a port to transmit traffic of multiple VLANs, you can configure the port as a trunk port.

You can configure a common Ethernet L2 interface or an aggregation port (AP) as a trunk port. For more information about AP, see *Link Aggregation Port*.

L2 switch ports have two key attributes, native VLAN and allowed VLAN. A trunk port has one native VLAN and several allowed VLANs.

- Native VLAN: When the trunk port receives an untagged packet or a priority packet, the trunk port considers that the packet comes from the native VLAN of this port. Packets of the native VLAN sent by the trunk port are untagged. When you configure a trunk link, ensure that the trunk ports of the link are bound to the same native VLAN.
- Allowed VLAN: When the trunk port receives a tagged packet, it determines whether the packet comes from an allowed VLAN of this port. If yes, the trunk port receives the packet. Otherwise, the trunk port discards the packet. Packets of an allowed VLAN sent by the trunk port are tagged.

1.6.2 Restrictions and Guidelines

- Before you configure the native VLAN and allowed VLANs for the trunk port, create these VLANs first. *When you* set the native VLAN to an inexistent VLAN, this VLAN is not created automatically.
- *vlan-list* can contain one or more VLANs. VLAN IDs are separated by commas (,). Continuous VLAN IDs are represented by connecting the first and the last VLAN IDs with a hyphen (-), for example, 3, 10-20, and 22.

all: Indicates that the allowed VLAN list includes all supported VLANs.

add *vlan-list*: Adds a specified VLAN to the allowed VLAN list.

remove *vlan-list*: Removes a specified VLAN from the allowed VLAN list.

except *vlan-list*: Adds all VLANs other than a specified VLANs to the allowed VLAN list.

only *vlan-list* : Adds only a specified VLAN to the allowed VLAN list and remove all the other VLANs from the list.

- The native VLAN of an interface can be excluded from the allowed VLAN list for this interface. In this case, traffic of the native VLAN cannot pass through this interface.
- You can run the **no switchport mode** command to restore the trunk port to an access port.

  You can run the **no switchport trunk native vlan** command to restore the native VLAN of the trunk port to a default value.

  You can run the **no switchport trunk allowed vlan** command to restore the allowed VLANs of the trunk port to default values.

1.6.3 Prerequisites

The interface to be configured must be an L2 interface. You can run the **show interface switchport** command to query the interface type. If the **Switchport** field corresponding to the interface is set to **enabled**, this interface is an L2 interface. Otherwise, this interface is an L3 interface. You should run the **switchport** command to configure the interface as an L2 interface and then set the default interface mode to **access**.

1.6.4 Procedure

(1) Create a VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create one VLAN or a group of VLANs as the native VLAN and allowed VLANs of the trunk port.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the interface as a trunk port.

a Enter the interface configuration mode.

interface *interface-type interface-number*

b Configure the L2 interface as a trunk port.

switchport mode trunk

The L2 interface mode is **access** by default.

(3) (Optional) Configure a native VLAN for the trunk port.

switchport trunk native vlan *vlan-id*

The native VLAN of the trunk port is VLAN 1 by default.

(4) (Optional) Configure an allowed VLAN list for the trunk port.

switchport trunk allowed vlan { **all** | { **add** | **remove** | **except** | **only** } *vlan-list* }

The allowed VLANs of the trunk port are VLANs 1 to 4094 by default.

1.7 Configuring Uplink Port

1.7.1 Overview

You can configure an interface as an uplink port to transmit only tagged frames of multiple VLANs. An uplink port has one native VLAN and several allowed VLANs.

The uplink port is generally used in QinQ scenarios as an interface for a PE to connect to a public network.

- Native VLAN: When the uplink port receives an untagged packet or a priority packet, the uplink port considers that the packet comes from the native VLAN of this port. Different from the trunk port, packets of the native VLAN sent by the uplink port are tagged.
- Allowed VLAN: When the uplink port receives a tagged packet, it determines whether the packet comes from the native VLAN of this port. If yes, the uplink port receives the packet. Otherwise, the uplink port discards the packet. Packets of the allowed VLANs sent by the uplink port are tagged.

1.7.2 Restrictions and Guidelines

- Before you configure the native VLAN and allowed VLANs for the uplink port, create these VLANs first.
- You can run the **no switchport mode** command to restore the uplink port to an access port.
- You can run the **no switchport trunk native vlan** command to restore the native VLAN of the uplink port to a default value.
- You can run the **no switchport trunk allowed vlan** command to restore the allowed VLANs of the uplink port to default values.
- You can run the **show vlan** [**id** *vlan-id*] and **show interface switchport** commands to check whether the configurations take effect.

1.7.3 Prerequisites

The interface to be configured must be an L2 interface. You can run the **show interface switchport** command to query the interface type. If the **Switchport** field corresponding to the interface is set to **enabled**, this interface is an L2 interface. Otherwise, this interface is an L3 interface. You should run the **switchport** command to configure the interface as an L2 interface and then set the default interface mode to **access**.

1.7.4 Procedure

(1) Create a VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create one VLAN or a group of VLANs as the native VLAN and allowed VLANs of the uplink port.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the interface as an uplink port.

a Enter the interface configuration mode.

interface *interface-type interface-number*

b Configure the L2 interface as an uplink port.

switchport mode uplink

The L2 interface mode is **access** by default.

(3) (Optional) Configure a native VLAN for the uplink port.

switchport trunk native vlan *vlan-id*

The native VLAN of the uplink port is VLAN 1 by default.

(4) (Optional) Configure an allowed VLAN list for the uplink port.

switchport trunk allowed vlan { **all** | { **add** | **remove** | **except** | **only** } *vlan-list* }

The allowed VLANs of the uplink port are VLANs 1 to 4094 by default.

1.8 Configuring Hybrid Port

1.8.1 Overview

You can configure an interface as a hybrid port to transmit traffic of multiple VLANs. The hybrid port is used in MAC VLANs and connected to an access link. A hybrid port has one native VLAN and several allowed VLANs.

- Native VLAN: The native VLAN of a hybrid port is VLAN 1 by default. When the hybrid port receives an untagged packet or a priority packet, the hybrid port considers that the packet comes from the native VLAN of this port. Packets of the native VLAN sent by the hybrid port are untagged.
- Allowed VLAN: The allowed VLANs of the hybrid port are VLANs 1 to 4094 by default. When the hybrid port receives a tagged packet, it determines whether the packet comes from an allowed VLAN of this port. If yes, the hybrid port receives the packet. Otherwise, the hybrid port discards the packet. Different from the trunk port, the hybrid port can send tagged or untagged packets of the allowed VLANs (other than the native VLAN) based on configurations.

1.8.2 Restrictions and Guidelines

- Before you configure the native VLAN and allowed VLANs for the hybrid port, create these VLANs first.
- You can run the **no switchport mode** command to restore the hybrid port to an access port.
- You can run the **no switchport hybrid native vlan** command to restore the native VLAN of the hybrid port to a default value.
- You can run the **no switchport hybrid allowed vlan** command to restore the allowed VLANs of the hybrid port to default values.
- You can run the **show vlan** [**id** *vlan-id*] and **show interface switchport** commands to check whether the configurations take effect.

1.8.3 Prerequisites

The interface to be configured must be an L2 interface. You can run the **show interface switchport** command to query the interface type. If the **Switchport** field corresponding to the interface is set to **enabled**, this interface is an L2 interface. Otherwise, this interface is an L3 interface. You should run the **switchport** command to configure the interface as an L2 interface and then set the default interface mode to **access**.

1.8.4 Procedure

(1) Create a VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create one VLAN or a group of VLANs as the native VLAN and allowed VLANs of the hybrid port.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the interface as a hybrid port.

a Enter the interface configuration mode.

interface *interface-type interface-number*

b Configure the L2 interface as a hybrid port.

switchport mode hybrid

The L2 interface mode is **access** by default.

(3) Configure a native VLAN for the hybrid port.

switchport hybrid native vlan *vlan-id*

The native VLAN of the hybrid port is VLAN 1 by default.

(4) Configure an allowed VLAN list for the hybrid port.

switchport hybrid allowed vlan { [**add**] **tagged** | [**add**] **untagged** | **only tagged** | **remove** } *vlan-list*

By default, the allowed VLANs of the hybrid port are tagged VLANs 2 to 4094 and untagged VLAN 1.

1.9 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

This section also describes the **debug** command used for outputting debugging information.

Caution

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

You can run the **clear** commands to clear information.

Caution

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

Table 1-3 Monitoring

Command	Purpose
show vlan [**id** *vlan-id*]	Displays VLAN configurations.
show interface switchport	Displays configurations of switch ports.
debug bridge vlan	Enables the debug function of a VLAN.

1.10 Configuration Examples

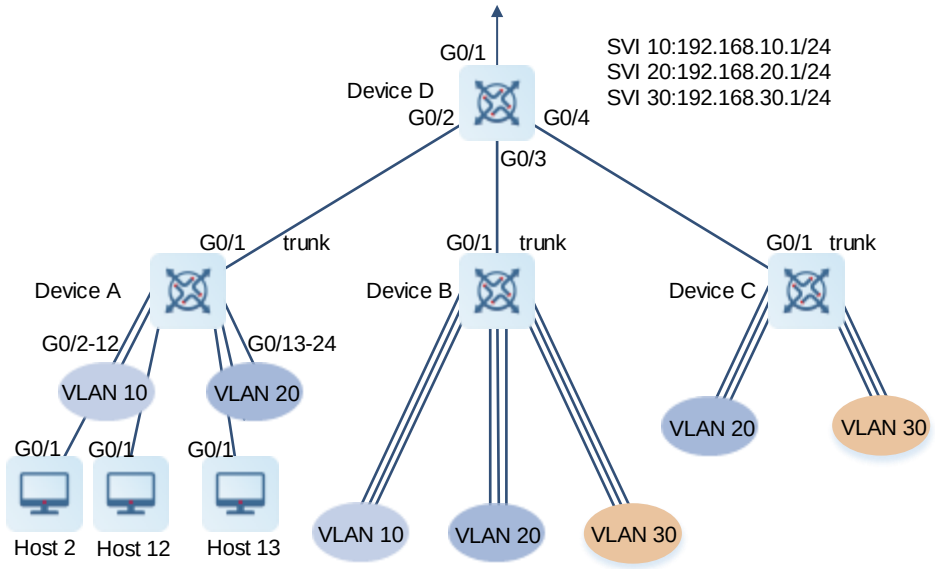
1.10.1 Configuring L2 Isolation and L3 Interconnection of VLAN

1. Requirements

The LAN of a user needs to be divided into VLAN 10, VLAN 20 and VLAN 30 to realize L2 isolation. The three VLANs correspond to the IP subnets 192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24, respectively, and these VLANs implement subnet interconnection based on the IP forwarding capability of L3 core switches.

2. Topology

Figure 1-15 Typical Scenario



3. Notes

The following describes the configuration procedure by using Device D and Device A as examples:

- On the L3 core device Device D, configure the three VLANs, configure the ports for connecting Device A, Device B, and Device C as trunk ports, and specify an allowed VLAN list to realize L2 isolation.
- Configure three SVIs on Device D, which are used as the gateway interfaces of the IP subnets corresponding to the three VLANs. Configure the IP addresses for these SVIs. Configure a default gateway for hosts based on the VLANs of the hosts.
- Create the VLANs separately on the three access devices, assign an access port for each VLAN, and configure the ports for connecting Device D as trunk ports.

4. Procedure

(1) Create and configure VLANs.

Create VLANs on Device D and rename VLAN 10.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# vlan 10
DeviceD(config-vlan)# name office
DeviceD(config-vlan)# vlan range 20,30
DeviceD(config-vlan-range)# exit
```

Create VLANs on Devices A, B and C. The following example describes how to configure Device A. For the configuration of Devices B and C, see the configuration procedure of Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan rang 10,20
DeviceA(config-vlan-range)# exit
```

(2) Configure IP addresses for the L3 SVIs of the VLANs on Device D.

```
DeviceD(config)# interface vlan 10
DeviceD(config-if-VLAN 10)# ip address 192.168.10.1 255.255.255.0
DeviceD(config-if-VLAN 10)# interface vlan 20
DeviceD(config-if-VLAN 20)# ip address 192.168.20.1 255.255.255.0
DeviceD(config-if-VLAN 20)# interface vlan 30
DeviceD(config-if-VLAN 30)# ip address 192.168.30.1 255.255.255.0
DeviceD(config-if-VLAN 30)# exit
```

(3) Configure specific types of ports and add the ports to the VLANs.

Configure the downlink port of Device D as a trunk port and configure an allowed VLAN list for the port.

```
DeviceD(config)# interface range gigabitethernet 0/2-4
DeviceD(config-if-range)# switchport
DeviceD(config-if-range)# switchport mode trunk
DeviceD(config-if-range)# exit
DeviceD(config)# interface gigabitethernet 0/2
DeviceD(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan remove
1-4094
```

```
DeviceD(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan add 10,20
DeviceD(config-if-GigabitEthernet 0/2)# interface gigabitethernet 0/3
DeviceD(config-if-GigabitEthernet 0/3)# switchport trunk allowed vlan only
10,20,30
DeviceD(config-if-GigabitEthernet 0/3)# interface gigabitethernet 0/4
DeviceD(config-if-GigabitEthernet 0/4)# switchport trunk allowed vlan only 20,30
DeviceD(config-if-GigabitEthernet 0/4)# end
DeviceD# write
```

Configure the uplink port of the access device as a trunk port. If you do not configure an allowed VLAN list for the port, the port allows packets of all VLANs to pass through by default. The following example describes how to configure Device A. For the configuration of Devices B and C, see the configuration procedure of Device A.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Configure the downlink port of the access device as an access port and add the port to a specified VLAN. The following example describes how to configure Device A. For the configuration of Devices B and C, see the configuration procedure of Device A.

```
DeviceA(config)# interface range gigabitethernet 0/2-12
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode access
DeviceA(config-if-range)# switchport access vlan 10
DeviceA(config-if-range)# interface range gigabitethernet 0/13-24
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode access
DeviceA(config-if-range)# switchport access vlan 20
DeviceA(config-if-range)# end
DeviceA# write
```

5. Verification

(1) Run the **show vlan** [**id** *vlan-id*] command on Device D to display VLAN information, including the VLAN ID, name, status and ports.

```
DeviceD# show vlan
VLAN  Name      Status             Ports
---- --------  --------   -------------------------------
   1 VLAN0001   STATIC    Gi0/1, Gi0/5, Gi0/6, Gi0/7
                       Gi0/8, Gi0/9, Gi0/10, Gi0/11
                       Gi0/12, Gi0/13, Gi0/14, Gi0/15
                       Gi0/16, Gi0/17, Gi0/18, Gi0/19
                       Gi0/20, Gi0/21, Gi0/22, Gi0/23
                       Gi0/24
  10 office    STATIC     Gi0/2, Gi0/3
  20 VLAN0020  STATIC     Gi0/2, Gi0/3, Gi0/4
  30 VLAN0030  STATIC     Gi0/3, Gi0/4
```

(2) Check the port configuration and port status.

Run the **show interface switchport** command on Device D to display the VLAN status of ports.

```
DeviceD# show interface gigabitethernet 0/2 switchport
Interface                    Switchport Mode     Access Native Protected VLAN
lists
------------------------------- ---------- --------- ------ ------ --------- --
GigabitEthernet 0/2            enabled   TRUNK    1    1      Disabled  10,20

DeviceD# show interface switchport
Interface                    Switchport Mode     Access Native Protected VLAN
lists
------------------------------- ---------- --------- ------ ------ --------- --
GigabitEthernet 0/2            enabled   TRUNK    1    1      Disabled  10,20
GigabitEthernet 0/3            enabled   TRUNK    1    1      Disabled
10,20,30
GigabitEthernet 0/4            enabled   TRUNK    1    1      Disabled  20,30
```

Run the **show interface description** command on Device D to check whether the port status is up.

```
DeviceD# show interface description
Interface                           Status   Administrative Description
---------------------------------------- -------- -------------- -----------
GigabitEthernet 0/2                   up      up
GigabitEthernet 0/3                   up      up
GigabitEthernet 0/4                   up      up

VLAN 10                              up      up
VLAN 20                              up      up
VLAN 30                              up      up
```

(3) Run the **show ip route** command on Device D to display the direct route information of SVIs.

Packets whose destination IP address matches 192.168.10.0/24 are forwarded to VLAN 10. Packets whose destination IP address matches 192.168.20.0/24 are forwarded to VLAN 20. Packets whose destination IP address matches 192.168.30.0/24 are forwarded to VLAN 30.

```
DeviceD# show ip route
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, A - Arp to host
       LA - Local aggregate route
       * - candidate default

Gateway of last resort is no set
…
C    192.168.10.0/24 is directly connected, VLAN 10
C    192.168.10.1/32 is local host.
C    192.168.20.0/24 is directly connected, VLAN 20
```

```
C    192.168.20.1/32 is local host.
C    192.168.30.0/24 is directly connected, VLAN 30
C    192.168.30.1/32 is local host.
```

Ping the SVI address of a VLAN (for example, VLAN 10) on Device D.

```
DeviceD# ping 192.168.10.1
Sending 5, 100-byte ICMP Echoes to 192.168.10.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

(4) The following example describes how to ping Hosts 2, 12, and 13.

Configure the default gateway of Host 2 in VLAN 10 as 192.168.10.1, the IP address of the port as 192.168.10.2, and the mask as 255.255.255.0.

```
Host2> enable
Host2# configure terminal
Host2(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.1
Host2(config)# interface gigabitethernet 0/1
Host2(config-if-GigabitEthernet 0/1)# no switchport
Host2(config-if-GigabitEthernet 0/1)# ip address 192.168.10.2 255.255.255.0
```

Configure the default gateway of Host 12 in VLAN 10 as 192.168.10.1, the IP address of the port as 192.168.10.12, and the mask as 255.255.255.0.

```
Host2> enable
Host2# configure terminal
Host2(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.1
Host2(config)# interface gigabitethernet 0/1
Host2(config-if-GigabitEthernet 0/1)# no switchport
Host2(config-if-GigabitEthernet 0/1)# ip address 192.168.10.12 255.255.255.0
```

Configure the default gateway of Host 13 in VLAN 20 as 192.168.20.1, the IP address of the port as 192.168.20.13, and the mask as 255.255.255.0.

```
Host13> enable
Host13# configure terminal
Host13(config)# ip route 0.0.0.0 0.0.0.0 192.168.20.1
Host13(config)# interface gigabitethernet 0/1
Host13(config-if-GigabitEthernet 0/1)# no switchport
Host13(config-if-GigabitEthernet 0/1)# ip address 192.168.20.13 255.255.255.0
```

Run the **show ip route** command on the hosts to display the default gateway. The default gateway must be configured on the transmit and receive ends. Inter-VLAN communication fails to be implemented if either end is not configured with the default gateway. Take Host 2 as an example. Due to the default route S*0.0.0.0/0 [1/0] via 192.168.10.1, a host sends a packet to the gateway 192.168.10.1 when the host tries to communicate across VLANs.

```
Host2# show ip route
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, A - Arp to host
       LA - Local aggregate route
       * - candidate default

Gateway of last resort is 192.168.10.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 192.168.10.1
C     192.168.10.0/24 is directly connected, GigabitEthernet 0/1
C     192.168.10.2/32 is local host.
```

Ping the IP address of a host (for example, Host 2) on Device D.

```
DeviceD# ping 192.168.10.2
Sending 5, 100-byte ICMP Echoes to 192.168.10.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/4 ms.
```

Hosts in the same VLAN (for example, VLAN 10) can ping each other.

```
Host2# ping 192.168.10.12
Sending 5, 100-byte ICMP Echoes to 192.168.10.12, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms.
```

Hosts in different VLANs can also ping each other. If you delete the IP address of an SVI on Device D or delete the default gateway on a host, hosts in different VLANs cannot ping each other.

```
Host2# ping 192.168.20.13
Sending 5, 100-byte ICMP Echoes to 192.168.10.3, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms.
```

6. Configuration Files

- Device D configuration file

```
vlan 10
 name office
vlan range 1,20,30

interface GigabitEthernet 0/2
 switchport mode trunk
 switchport trunk allowed vlan only 10,20
interface GigabitEthernet 0/3
 switchport mode trunk
 switchport trunk allowed vlan only 10,20,30
interface GigabitEthernet 0/4
 switchport mode trunk
```

```
 switchport trunk allowed vlan only 20,30

interface VLAN 10
 ip address 192.168.10.1 255.255.255.0
interface VLAN 20
 ip address 192.168.20.1 255.255.255.0
interface VLAN 30
 ip address 192.168.30.1 255.255.255.0
```

- Device A configuration file. Similar configurations of ports are represented by ellipsis (...). For the configuration of Devices B and C, see the Device A configuration procedure.

```
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport access vlan 10
…
interface GigabitEthernet 0/12
 switchport access vlan 10
!
interface GigabitEthernet 0/13
 switchport access vlan 20
…
interface GigabitEthernet 0/24
 switchport access vlan 20
```

7. Common Errors

- If no IP address is configured for a gateway (SVI), or no default gateway is configured for an STA, or either the transmit or receive end is not configured with the default gateway, STAs in different VLANs cannot ping each other.
- If connected trunk ports have different native VLANs, data communication may fail.
- If interfaces connected to STAs are not configured as access ports, data communication may fail.
- If only one VLAN needs to be configured for a trunk port but the default allowed VLAN of the trunk port is not deleted after the VLAN creation command is run, the configuration result is inconsistent with the configuration plan.
- A trunk port on a vendor's device needs to receive only tagged frames and discard untagged packets. If the trunk port of the local device sends untagged packets of the native VLAN, the packets may be discarded. In this case, configure the connection port on the local device as an uplink port so that packets sent by this port are tagged.

Contents

1 Configuring Private VLAN 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Basic Concepts 1

1.1.3 L2 Forwarding and Isolation of PVLAN 3

1.1.4 Cross-Device L2 Application of PVLAN 4

1.1.5 L3 Application of PVLAN on a Single Device 4

1.2 Monitoring 5

1 Configuring Private VLAN

1.1 Introduction

1.1.1 Overview

Carriers hope to isolate users to authenticate and charge each user, avoid virus attacks and broadcast storms, and strengthen user security. VLANs are isolated at L2. If each user is assigned with a VLAN, the authentication, billing, and security requirements can be met. However, a device supports 4094 VLANs at most. Assigning a VLAN to each user limits the number of users supported by a device. What's more, it is infeasible for an L3 device to assign one IP address to each VLAN in consideration of scarce IP addresses. To solve the problem, the private VLAN (PVLAN) technology is developed.

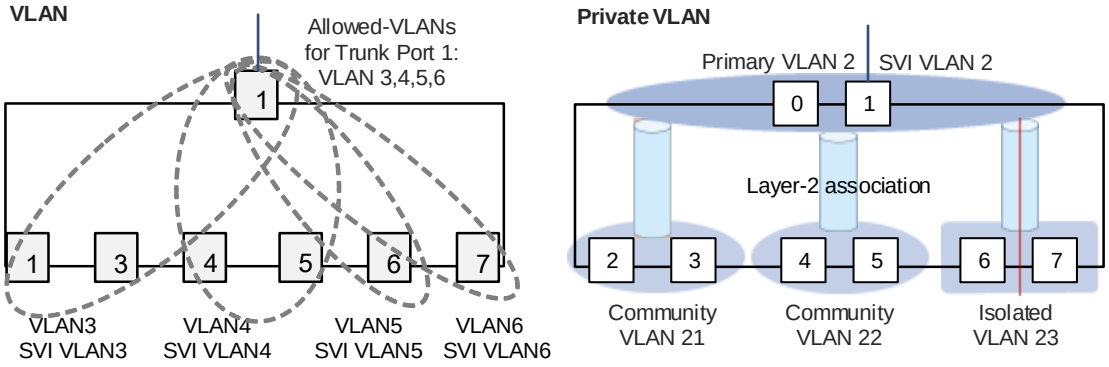
1.1.2 Basic Concepts

The PVLAN technology divides an L2 broadcast domain of a VLAN into multiple sub-domains to form a dual-layer VLAN structure. The outer layer is referred to as primary VLAN, and the inner layer is referred to as secondary VLAN. Secondary VLANs can be further divided to community VLANs and isolated VLANs.

1. Features

- You can configure multiple PVLANs on a device. A PVLAN is a PVLAN domain.
- Each PVLAN can contain only one primary VLAN and multiple secondary VLANs. The primary VLAN corresponds to multiple secondary VLANs. The primary VLAN and one secondary VLAN form a PVLAN pair, which represents a PVLAN sub-domain. For example, VLAN 2/21 represents a PVLAN sub-domain. A PVLAN domain can have multiple PVLAN sub-domains. The secondary VLANs of different sub-domains are different, but they share the same primary VLAN.
- Both the primary VLAN and secondary VLANs can contain physical ports. As shown in Figure 1-1, ports 0 and 1 belong to primary VLAN 2; and ports 2 and 3 belong to community VLAN 21. After an L2 association is configured between primary VLAN 2 and community VLAN 21, ports 0, 1, 2, and 3 belong to the same PVLAN sub-domain VLAN 2/21. They can make L2 communication with each other.
- In a PVLAN, L3 switch virtual interfaces (SVIs) can be created only in the primary VLAN, and L3 SVIs cannot be created in secondary VLANs. Hosts in a secondary VLAN can make L3 communication only after an L3 association is configured between the secondary VLAN and the primary VLAN. Otherwise, the hosts can make only L2 communication.

Figure 1-1 Logic Diagram of PVLAN



2. Primary VLAN and Promiscuous Port

Physical ports belonging to the primary VLAN are referred to as promiscuous ports. A PVLAN can have one or more promiscuous ports.

- In a PVLAN domain, a promiscuous port can communicate with any port, including another promiscuous port, a community VLAN port, and an isolated VLAN port. A promiscuous port is used as an uplink port for connecting to an external network or a port for connecting to a shared server so that hosts in all secondary VLANs can access the network and shared server.
- Outside a PVLAN domain, a promiscuous port belongs to the primary VLAN, allows common packets with the primary VLAN ID to pass through, and discards the other common VLAN packets.

3. Community VLAN and Community Port

A PVLAN domain can have multiple community VLANs. The ports in a community VLAN are referred to as community ports.

- Community ports in a community VLAN can communicate with each other but community ports of different community VLANs cannot communicate with each other.
- Community ports can communicate with promiscuous ports.
- Community ports cannot communicate with isolated ports.

4. Isolated VLAN and Isolated Port

A PVLAN domain can have only one isolated VLAN. Ports in an isolated VLAN are referred to as isolated ports.

- Isolated ports cannot communicate with each other. You can assign required hosts to an isolated VLAN for isolation.
- Isolated ports can communicate with only promiscuous ports. Packets can be forwarded from isolated ports to the promiscuous ports and vice versa.
- Packets can be forwarded from an isolated port to a trunk port. When receiving a packet (packet from the promiscuous port) with the VLAN ID of the primary VLAN ID, the trunk port can forward the packet to the isolated port. This enables the isolated port to communicate with an external network through a promiscuous port. Hosts in an isolated VLAN cannot communicate with each other. Therefore, when receiving a packet with the VLAN ID of the isolated VLAN, the trunk port cannot forward the packet to the isolated port.

Caution

Ports in a PVLAN can be used as mirroring source ports but cannot be used as mirroring destination ports.

1.1.3 L2 Forwarding and Isolation of PVLAN

Table 1-1 lists packet forwarding rules between different types of ports and VLAN tag changes.

Table 1-1 Packet Forwarding Rules between Different Types of Ports and VLAN Tag Changes

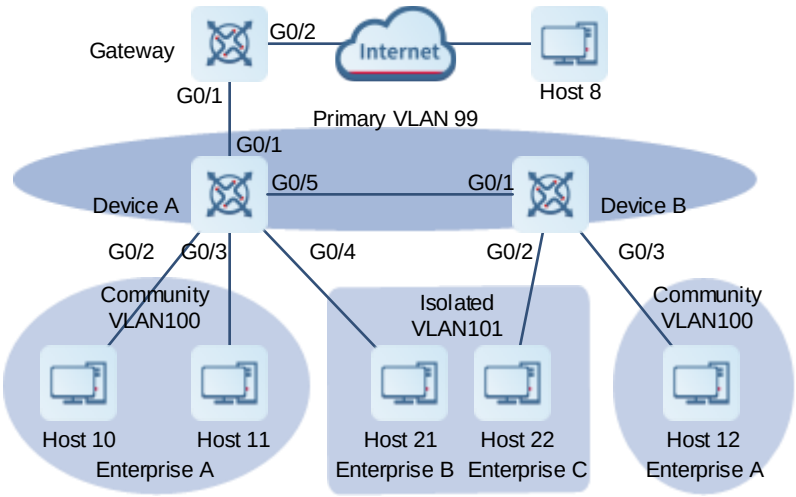
Output Port / Input Port	Promiscuous Port	Community Port	Isolated Port	Trunk Port (in the Same VLAN)
Promiscuous Port	Reachable, VLAN tag unchanged	Reachable, VLAN tag unchanged	Reachable, VLAN tag unchanged	Reachable, a primary VLAN tag added
Community Port	Reachable, VLAN tag unchanged	Reachable in the same community VLAN, VLAN tag unchanged Unreachable in different community VLANs	Unreachable	Reachable, a community VLAN tag added
Isolated Port	Reachable, VLAN tag unchanged	Unreachable	Unreachable	Reachable, an isolated VLAN tag added
Trunk Port	Reachable, VLAN tag removed	Reachable in the primary VLAN, VLAN tag removed Reachable in the same community VLAN, VLAN tag removed Unreachable in different community VLANs Unreachable in an isolated VLAN	Reachable in the primary VLAN, VLAN tag removed Unreachable in a community VLAN Unreachable in an isolated VLAN	Reachable, VLAN tag unchanged
Switch CPU	Reachable, no VLAN tag	Reachable, no VLAN tag	Reachable, no VLAN tag	Reachable, a primary VLAN tag added

1.1.4 Cross-Device L2 Application of PVLAN

As shown in the following figure, in the hosting service operation network, enterprise hosts are connected to the network through Device A or Device B. Hosts of an enterprise can communicate with each other but the host communication between enterprises is isolated. All the enterprise hosts share the same gateway address and can communicate with the external network through this gateway address. The deployment mode is as follows:

- Configure the PVLAN function on Device A and Device B, and add all enterprise hosts to the same PVLAN, for example, primary VLAN 99. All the enterprise hosts communicate with an external network through a shared L3 interface of the primary VLAN 99. The external network perceives the primary VLAN 99 only and does not perceive secondary VLANs. Configure GigabitEthernet 0/5 of Device A and GigabitEthernet 0/1 of Device B as trunk ports.
- If an enterprise has multiple hosts, allocate the hosts to different community VLANs and configure the ports connected to the hosts as host ports of the community VLANs so that the hosts in the enterprise can communicate with each other but host communication between enterprises is isolated.
- If an enterprise has only one host, allocate the host to an isolated VLAN and configure the port connected to the host as the host port of the isolated VLAN, to implement isolation of communication between hosts of different enterprises.
- Connect GigabitEthernet 0/1 of Device A to the gateway and configure this interface as a promiscuous port. The promiscuous port allows only packets with the primary VLAN ID to pass through and outputs untagged packets.
- Configure GigabitEthernet 0/1 of the gateway as a trunk or hybrid port. Because packets forwarded by a promiscuous port do not carry tags, set the native VLAN of GigabitEthernet 0/1 of the gateway to the primary VLAN of the PVLAN.

Figure 1-2 Typical Network Topology of PVLAN Applied Across L2 Devices



1.1.5 L3 Application of PVLAN on a Single Device

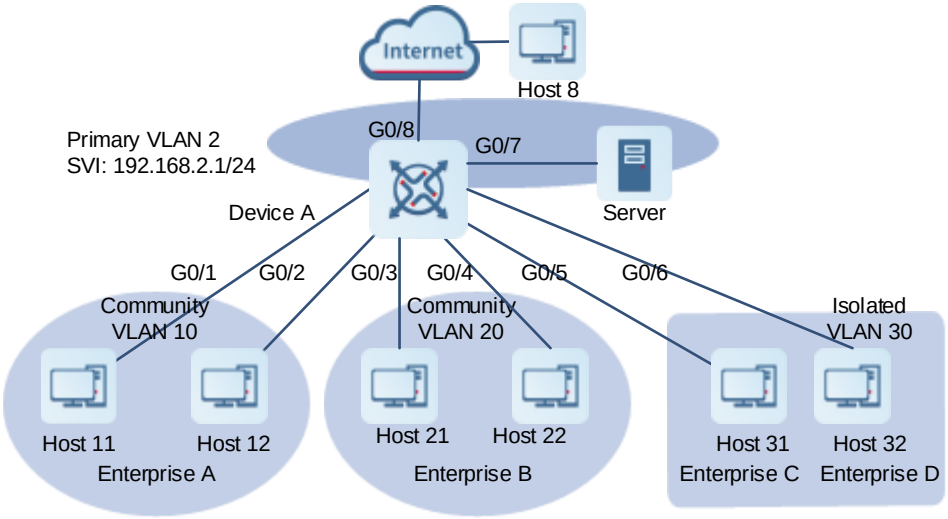
As shown in the following figure, in the hosting service operation network, enterprise hosts are connected to the network through the L3 Device A. Hosts of an enterprise can communicate with each other but the host communication between enterprises is isolated. All enterprise hosts can access the server. All enterprise hosts

share the same gateway address and can communicate with the external network through this gateway address.

The deployment mode is as follows:

- Add all enterprise hosts to the same PVLAN, for example, primary VLAN 2. Assign hosts of enterprise A to community VLAN 10, hosts of enterprise B to community VLAN 20, and hosts of enterprises C and D to isolated VLAN 30.
- Configure GigabitEthernet 0/7 that is directly connected to the server as a promiscuous port. Then, all enterprise hosts can communicate with the server through the promiscuous port.
- Configure the gateway address of the PVLAN on the L3 Device A (in this example, set the SVI address of VLAN 2 to 192.168.2.1/24) and configure the mappings between the primary VLAN and the secondary VLANs on the L3 interface. Then, all enterprise hosts can communicate with the external network through this gateway address.

Figure 1-3 Typical Network Topology of PVLAN Applied on a Single L3 Device



1.2 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

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

Run the **clear** commands to clear information.

Caution

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

Table 1-2 Monitoring

Command	Purpose
show vlan private-vlan	Displays PVLAN configuration.
debug bridge pvlan	Debugs the PVLAN function.

Contents

1 Configuring Super VLAN 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Background and Function 1
1.1.3 Principles 3
1.2 Configuration Task Summary 5
1.3 Configuring L2 Association for a Super VLAN 6
1.3.1 Overview 6
1.3.2 Restrictions and Guidelines 6
1.3.3 Procedure 6
1.4 Configuring L3 Communication for a Super VLAN 7
1.4.1 Overview 7
1.4.2 Restrictions and Guidelines 7
1.4.3 Procedure 7
1.5 Configuring an IP Address Range for a Sub VLAN 8
1.5.1 Overview 8
1.5.2 Restrictions and Guidelines 8
1.5.3 Procedure 8
1.6 Configuring a Broadcast VLAN 9
1.6.1 Overview 9
1.6.2 Restrictions and Guidelines 9
1.6.3 Procedure 9

1.7 Monitoring 9

1.8 Configuration Examples..... 10

1.8.1 Configuring Super VLAN 10

1 Configuring Super VLAN

1.1 Introduction

1.1.1 Overview

Super virtual local area network (VLAN), also referred to as VLAN aggregation, is a VLAN assignment method.

A common VLAN corresponds to a subnet and is used to complete L3 communication with another VLAN based on a gateway IP address.

The super VLAN technology allows you to configure common VLANs as sub VLANs, aggregate them into one super VLAN, assign only one IP address to the super VLAN as the gateway IP address to implement inter-VLAN L3 communication. This technology saves IP address resources and facilitates network management.

1.1.2 Background and Function

1. Background

A common VLAN corresponds to a logical subnet and is isolated from other VLANs at L2. Each subnet must be assigned with a gateway IP address to implement inter-VLAN L3 communication. In addition to the gateway IP address, each subnet also requires a subnet ID and a subnet-directed broadcast IP address as dedicated addresses. These three addresses cannot be assigned to hosts.

Suppose that a local area network (LAN) covers three departments and therefore requires three VLANs. The VLAN IDs and hosts of the three departments are as follows: VLAN 10 (31 hosts), VLAN 20 (44 hosts), and VLAN 30 (128 hosts). There are 203 hosts in total. The network segment 192.168.1.0/24 has 256 IP addresses, which are assigned to the three departments to meet network requirements. A device performs a logical "AND" operation on IP addresses and subnet masks in binary format to identify the subnet, to which the hosts belong. The VLAN assignment result is as follows:

- VLAN 10 requires 31 host addresses and 3 dedicated addresses, totaling 34 addresses. VLAN 10 needs to be assigned with 64 IP addresses (2^6) with the subnet mask of /26.

  IP address range: 192.168.1.0 to 192.168.1.63 = 11000000.10101000.00000001.(00000000 to 00111111)

  Subnet mask (/26): 255.255.255.192 = 11111111.11111111.11111111.11000000

  Network ID obtained via logical "AND" operation in binary format: 192.168.1.0 = 11000000.10101000.00000001.00000000

  Gateway IP address: 192.168.1.1 = 11000000.10101000.00000001.00000001

  Subnet-directed broadcast IP address: 192.168.1.63 = 11000000.10101000.00000001.00111111

  Host IP address: 192.168.1.2 to 192.168.1.62 (31 hosts must be assigned with 61 addresses, and therefore 30 addresses are wasted)

- VLAN 20 requires 44 host addresses and 3 dedicated addresses, totaling 47 addresses. VLAN 20 needs to be assigned with 64 addresses (2^6) with the subnet mask of /26.

  IP address range: 192.168.1.64 to 192.168.1.127 = 11000000.10101000.00000001.(01000000 to 01111111)

Subnet mask (/26): 255.255.255.192 = 11111111.11111111.11111111.11000000

Network ID obtained via logical "AND" operation in binary format: 192.168.1.64 = 11000000.10101000.00000001.01000000

Gateway IP address: 192.168.1.65 = 11000000.10101000.00000001.01000001

Subnet-directed broadcast IP address: 192.168.1.127 = 11000000.10101000.00000001.01111111

Host IP address: 192.168.1.66 to 192.168.1.126 (44 hosts must be assigned with 61 addresses, and therefore 17 addresses are wasted)

- Only 125 addresses are available to VLAN 30 that includes 128 hosts.

  IP address range: 192.168.1.128 to 192.168.1.255 = 11000000.10101000.00000001.(10000000 to 11111111)

  Subnet mask (/25): 255.255.255.128 = 11111111.11111111.11111111.10000000

  Network ID obtained via logical "AND" operation in binary format: 192.168.1.128 = 11000000.10101000.00000001.10000000

  Gateway IP address: 192.168.1.129 = 11000000.10101000.00000001.10000001

  Subnet-directed broadcast IP address: 192.168.1.255 = 11000000.10101000.00000001.11111111

  Host IP address: 192.168.1.130 to 192.168.1.254 (128 hosts are assigned with only 125 addresses)

It can be inferred from the assignment method that if each VLAN is assigned with a subnet, 9 dedicated addresses are required and 47 (30 + 17) host addresses are wasted. Though the network segment 192.168.1.0/24 contains 256 addresses, they cannot meet the IP address requirements of the 203 hosts.

This assignment method also lacks flexibility. If you add hosts to VLAN 20, exceeding the limit 64, you have to add the new hosts to another VLAN and assign IP addresses of another network segment to the new hosts unless you change the original IP address assignment policy. As a result, hosts from the same department do not belong to the same network segment.

To avoid the IP address waste and address assignment management problems, the super VLAN technology is developed.

2. Function

The super VLAN technology is used to aggregate multiple sub VLANs into one super VLAN.

L2 isolation is implemented by sub VLANs, and L3 interconnection is implemented by super VLANs.

A super VLAN corresponds to a logical subnet, and all sub VLANs in the super VLAN belong to this subnet and share the same network ID, gateway IP address, and subnet-directed broadcast IP address. This saves IP address resources and improves network management flexibility.

3. Features

- Super VLAN

  A super VLAN corresponds to a network segment. Switch virtual interfaces (SVIs) can be created only in super VLANs, but no physical port can be added to the super VLANs. Super VLAN manages inter-VLAN communication of sub VLANs by using the SVIs. A super VLAN cannot be considered as an IEEE 802.1Q VLAN. A super VLAN has only L3 attributes of a common VLAN.

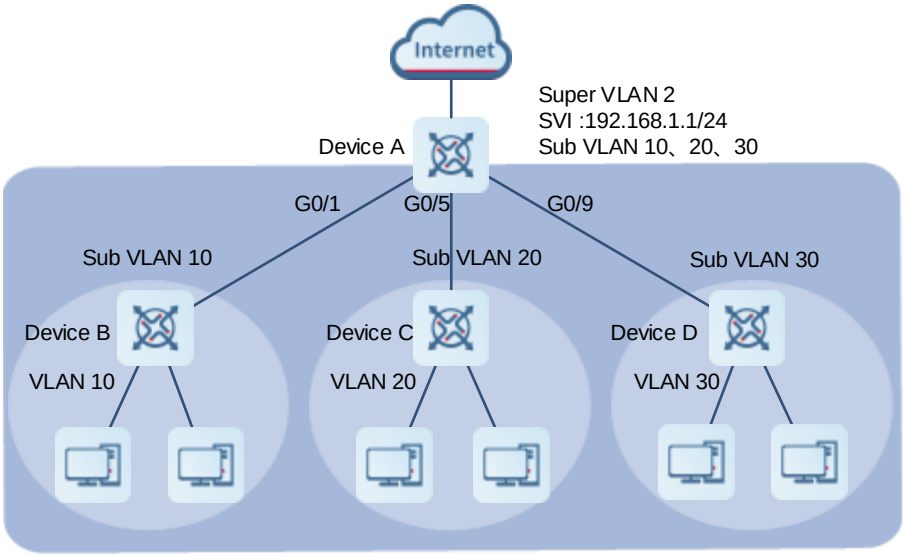
- Sub VLAN

Each sub VLAN is an independent broadcast domain, and is isolated from other sub VLANs at L2. A sub VLAN belongs to only one super VLAN. No SVI can be created in a sub VLAN, which can contain only physical ports. A sub VLAN has only L2 attributes of a common VLAN. To implement L3 communication across broadcast domains, sub VLANs must use the SVIs of the super VLAN.

4. Application

After the super VLAN technology is applied to the case described in Background, the network segment 192.168.1.0/24 can meet the requirement for IP addresses. As shown in Figure 1-1, on Device A, VLAN 2 is configured as a super VLAN, SVI address 192.168.1.1/24 as the gateway address, and VLAN 10, VLAN 20 and VLAN 30 as sub VLANs. Hosts are isolated at L2 through sub VLANs and make L3 communication with hosts in other network segments based on the common gateway IP address. The network segment accommodates IP addresses ranging from 192.168.1.2 to 192.168.1.254. A total of 253 IP addresses can be assigned to the 203 hosts in the sub VLANs, and there are some idle addresses left. Devices B, C, and D are used to expand the access ports and configured with VLAN 10, VLAN 20, and VLAN 30, respectively.

Figure 1-1 Application of Super VLAN



1.1.3 Principles

1. Communication in a Sub VLAN

A common VLAN corresponds to a subnet, and hosts in the subnet belong to the same broadcast domain. When a host (source host) in a common VLAN sends a packet, the host determines whether the destination host is in the same subnet as the source host. If yes, the host broadcasts an Address Resolution Protocol (ARP) request to request and obtain the MAC address of the destination host, and then completes L2 communication with the destination host. If not, the host broadcasts an ARP request to request and obtain the MAC address of the gateway, and then forwards the packet to the gateway for L3 communication.

In a super VLAN, when a host (source host) in a sub VLAN sends a packet, the host determines whether the destination host is in the same subnet as the source host and whether they belong to the same sub VLAN. If yes, the communication procedure is similar to the L2 communication procedure of a common VLAN. The communication steps are as follows:

(1) The source host determines that the destination host is in the same subnet as the source host but the destination MAC address is unknown. The source host broadcasts an ARP request to request the destination MAC address.

(2) A switch learns the MAC address and forwards the ARP broadcast request to all ports except the source port in the sub VLAN.

(3) Upon receiving the ARP request, the destination host in the sub VLAN sends a unicast ARP reply to the source host.

(4) The switch learns the MAC address and forwards the ARP reply packet.

(5) Upon receiving the ARP reply packet, the source host obtains the destination MAC address and then can realize L2 communication with the destination host.

2. Communication Between Different Sub VLANs in a Super VLAN

Though the sub VLANs in a super VLAN belong to the same subnet, they are isolated at L2 and belong to different broadcast domains. When a host (source host) in a sub VLAN tries to communicate with a host (destination host) in another sub VLAN of the super VLAN, the communication initially follows an L2 forwarding procedure because the source host does not know it is isolated from the destination host. In this case, communication between different sub VLANs relies on proxy ARP of a switch. The actual communication procedure is completed at L3. The communication steps are as follows.

(1) The source host determines that the destination host is in the same subnet as the source host but the destination MAC address is unknown. The source host broadcasts an ARP request to request the destination MAC address.

(2) A switch learns the source MAC address and forwards the ARP request to all ports except the source port in the sub VLAN.

(3) Hosts in other sub VLANs cannot receive this ARP request. Therefore, no ARP reply is sent to the switch. After a specified period of time, the switch enables proxy ARP, replaces the source MAC address in the request packet with the gateway MAC address of the super VLAN, and broadcasts the ARP request in all sub VLANs of the super VLAN to request the destination MAC address.

Note

- The IP addresses in sub VLANs may be discontinuous and dynamic due to the address assignment policy of a Dynamic Host Configuration Protocol (DHCP) server or capacity expansion. This makes the super VLAN unable to identify the sub VLAN, to which the destination IP address belongs. Therefore, the broadcast packet is sent to all sub VLANs in the super VLAN by default.
- You can configure an IP address range for each sub VLAN so that the broadcast packet can be sent to a specific sub VLAN based on the IP address. In this case, the DHCP function must be disabled, because the IP addresses assigned by this function may fall out of the IP address range of a specific sub VLAN. The configured static IP addresses must be within the IP address range of a specific sub VLAN. Otherwise, communication between sub VLANs cannot be realized.
- You can configure a sub VLAN as a broadcast VLAN so that broadcast packets sent by the super VLAN are destined to this sub VLAN. However, this configuration may cause the failure of the destination host to receive the ARP broadcast request, resulting in a communication exception.

(4) Upon receiving the ARP request, the destination host in another sub VLAN learns the mapping between the gateway MAC address and the source IP address and sends a unicast ARP reply to the gateway.

(5) The switch learns the following mapping of the destination host: "IP address – MAC address – sub VLAN – port". The switch replaces the destination MAC address with the gateway MAC address and sends the unicast ARP reply to the source host.

(6) Upon receiving the ARP reply, the source host regards the gateway MAC address as the destination MAC address, learns the mapping between the gateway MAC address and the destination IP address, and completes L3 communication through the proxy gateway.

The process in which the gateway replaces the source MAC address with the gateway MAC address to send an ARP request and the process in which the gateway replaces the destination MAC address with the gateway MAC address to send an ARP reply are referred to as proxy ARP. Communication across broadcast domains needs to rely on proxy ARP.

3. Communication Between Super VLANs

Different super VLANs correspond to different subnets and the destination host and source host in different super VLANs belong to different broadcast domains. The source host can determine that the destination host is in a different broadcast domain based on the IP address network segment. The communication process is similar to the communication between different network segments of common VLANs. In this communication procedure, the gateway also performs proxy ARP. However, the gateway is an SVI of the super VLAN rather than the SVI of a common VLAN.

4. Inter-Device L2 Communication

Super VLAN works at L3. The SVI of a super VLAN is used as a gateway only in L3 communication across broadcast domains (across network segments or in the same network segment). The VLAN ID of a super VLAN is not used in L2 communication.

No physical port can be added to a super VLAN. On a device where a super VLAN is configured, packets with containing VLAN ID of the super VLAN cannot pass through any port of the device.

As shown in Figure 1-1, VLAN 2 is configured as a super VLAN on Device A. Assume that VLAN 2 is configured as a common VLAN on Device B. When Device A receives a packet from VLAN 2 on Device B, Device A discards this packet.

The communication between sub VLAN 10 on Device A and VLAN 10 on Device B is inter-device L2 communication. Their connected interfaces must allow packets of sub VLAN 10 to pass so that the packets can be forwarded by the interface. If packets are tagged, the VLAN ID in the tags is the VLAN ID of sub VLAN 10.

1.2 Configuration Task Summary

The configuration includes the following tasks:

(1) Configure a super VLAN and sub VLANs.

a Configuring L2 Association for a Super VLAN

b Configuring L3 Communication for a Super VLAN

c (Optional) Configuring an IP Address Range for a Sub VLAN

d (Optional) Configuring a Broadcast VLAN

(2) Configure ports and add the ports to the sub VLANs. For more information, see *Configuring VLAN*.

1.3 Configuring L2 Association for a Super VLAN

1.3.1 Overview

You can configure a common VLAN as a super VLAN, configure other common VLANs as sub VLANs, and add the sub VLANs to the super VLAN. A sub VLAN is a broadcast domain, hosts in a sub VLAN can make L2 communication with each other but are L2 isolated from hosts outside the sub VLAN.

1.3.2 Restrictions and Guidelines

- Super VLAN
  - VLAN 1 cannot be configured as a super VLAN.
  - No physical port can be added to a super VLAN. After a common VLAN is configured as a super VLAN, the ports that have been added to the VLAN exit the VLAN and are added to VLAN 1.
  - A super VLAN does not belong to any physical port. Therefore, the device configured with the super VLAN cannot process packets that contain the super VLAN tag.
  - A super VLAN cannot be configured as a sub VLAN of another super VLAN. A sub VLAN of a super VLAN cannot be configured as a super VLAN.
  - You can use the **no supervlan** command to restore a super VLAN and all its sub VLANs to common VLANs. You must restore a super VLAN to a common VLAN before deleting this super VLAN by running the **no vlan** command.
- Sub VLAN
  - You must configure sub VLANs for a super VLAN so that the super VLAN is valid.
  - VLAN 1 cannot be configured as a sub VLAN.
  - You can configure multiple super VLANs on a device. A sub VLAN can be added to one super VLAN only and the sub VLANs in different super VLANs must be unique.
  - Avoid configuring too many sub VLANs. A broadcast packet of a super VLAN is sent to all its sub VLANs by default. The configuration of too many sub VLANs will degrade the performance.
  - Physical ports can be added to a sub VLAN. A common VLAN configured with an L3 SVI cannot be configured as a sub VLAN.
  - You must restore a sub VLAN to a common VLAN by running the **no subvlan** command before deleting this sub VLAN by running the **no vlan** command. In super VLAN configuration mode, you can use the **no subvlan** [*vlan-id-list*] command to restore a specific sub VLAN in the super VLAN to a common VLAN.

1.3.3 Procedure

(1) Create a common VLAN to be configured as a sub VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a common VLAN to be configured as a sub VLAN.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Create a common VLAN to be configured as a super VLAN and enter the VLAN configuration mode.

vlan *vlan-id*

Only VLAN 1 exists by default.

(3) Configure a common VLAN as a super VLAN.

supervlan

The super VLAN function is disabled by default. Therefore, created VLANs are common VLANs.

(4) Add the common VLAN to the super VLAN to make the common VLAN become a sub VLAN of the super VLAN.

subvlan *vlan-id-list*

No common VLAN is added to a super VLAN to become a sub VLAN by default.

1.4 Configuring L3 Communication for a Super VLAN

1.4.1 Overview

A super VLAN corresponds to a logical subnet. No physical port can be added to a super VLAN and only an L3 SVI can be configured for the super VLAN. IP addresses must be configured for L3 SVIs. Sub VLANs of a super VLAN share the gateway address of the super VLAN and reside in the same network segment.

Proxy ARP must be enabled on the super VLAN and sub VLANs so that hosts in the sub VLANs can implement L3 communication across broadcast domains through proxy ARP of the super VLAN.

1.4.2 Restrictions and Guidelines

- An SVI and an IP address must be configured for a super VLAN. The SVI is a virtual interface used for communication between sub VLANs. You cannot configure an SVI for a sub VLAN.
- When you configure an SVI for a super VLAN, the system assigns an L3 interface invisible to hosts to each sub VLAN in the super VLAN. The system may restore some sub VLANs to common VLANs due to resource deficiency. After an SVI is configured for a super VLAN, the attempt of adding sub VLANs may fail due to resource deficiency.
- Proxy ARP must be configured in VLAN configuration mode. Proxy ARP must be enabled on both the super VLAN and its sub VLANs so that L3 communication can be implemented. Proxy ARP is enabled by default. To isolate communication between sub VLANs, you can use the **no proxy-arp** command to disable proxy ARP.

1.4.3 Procedure

(1) Configure a gateway for a super VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create an SVI for the super VLAN and enter the SVI configuration mode.

interface vlan *vlan-id*

No SVI exists in a VLAN by default.

d Configure an IP address and a subnet mask for the gateway of the super VLAN.

ip address *ip-address mask*

No IP address is configured for an SVI by default.

e Return to the global configuration mode.

exit

(2) (Optional) Enable proxy ARP.

a Enter the VLAN configuration mode of the super VLAN and sub VLAN.

vlan { *vlan-id* | **range** *vlan-range* }

b Enable proxy ARP for the super VLAN and the sub VLAN.

proxy-arp

Proxy ARP is enabled for the super VLAN and the sub VLAN by default.

1.5 Configuring an IP Address Range for a Sub VLAN

1.5.1 Overview

The gateway IP address and subnet mask of a super VLAN jointly determine the subnet range. A super VLAN sends a broadcast packet to all sub VLANs in the super VLAN by default. To limit the broadcast range, you can configure an IP address range for each sub VLAN so that the super VLAN can send a broadcast packet to a specific sub VLAN based on an IP address range. The IP addresses of hosts must be within the IP address range of the local sub VLAN. Otherwise, the hosts cannot make L3 communication. Unless otherwise specified, you do not need to configure an IP address range for a sub VLAN.

1.5.2 Restrictions and Guidelines

- The IP address range of a sub VLAN must be within the gateway IP address range of the super VLAN that the sub VLAN belongs to.
- IP address ranges for different sub VLANs of a super VLAN cannot overlap.
- IP addresses (both static and dynamic IP addresses) of hosts in a sub VLAN must be within the IP address range of the sub VLAN. Otherwise, hosts in the sub VLAN cannot make L3 communication.
- The IP addresses assigned by the DHCP function may fall out of the IP address range you specify for a sub VLAN. If the IP addresses assigned by the DHCP function fall out of the specified IP address range, hosts in the sub VLAN cannot communicate with an external network. Therefore, you are not advised to configure an IP address range for a sub VLAN if DHCP is used to dynamically assign IP addresses to hosts.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the sub VLAN configuration mode.

vlan *vlan-id*

(4) Configure an IP address range for the sub VLAN.

subvlan-address-range *start-ip-address end-ip-address*

No IP address range is specified for a sub VLAN by default.

1.6 Configuring a Broadcast VLAN

1.6.1 Overview

A super VLAN sends a broadcast packet to all sub VLANs in the super VLAN by default. To limit the broadcast range, you can configure a sub VLAN as a broadcast VLAN so that broadcast packets of the super VLAN are sent in only this sub VLAN.

1.6.2 Restrictions and Guidelines

Only a sub VLAN of a super VLAN can be configured as a broadcast VLAN. Only one broadcast VLAN can be configured for a super VLAN. A later configured broadcast VLAN overwrites a previously configured broadcast VLAN.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the super VLAN configuration mode.

vlan { *vlan-id* | **range** *vlan-range* }

(4) Configure a broadcast VLAN.

bcast vlan *sub-vlan-id*

No broadcast VLAN exists by default. A super VLAN sends broadcast packets to all of its sub VLANs.

1.7 Monitoring

Run the **show** commands to check the running status of a configured function and verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

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

You can run the **clear** commands to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
show supervlan	Displays the super VLAN configuration.
debug bridge svlan	Debugs the super VLAN function.

1.8 Configuration Examples

1.8.1 Configuring Super VLAN

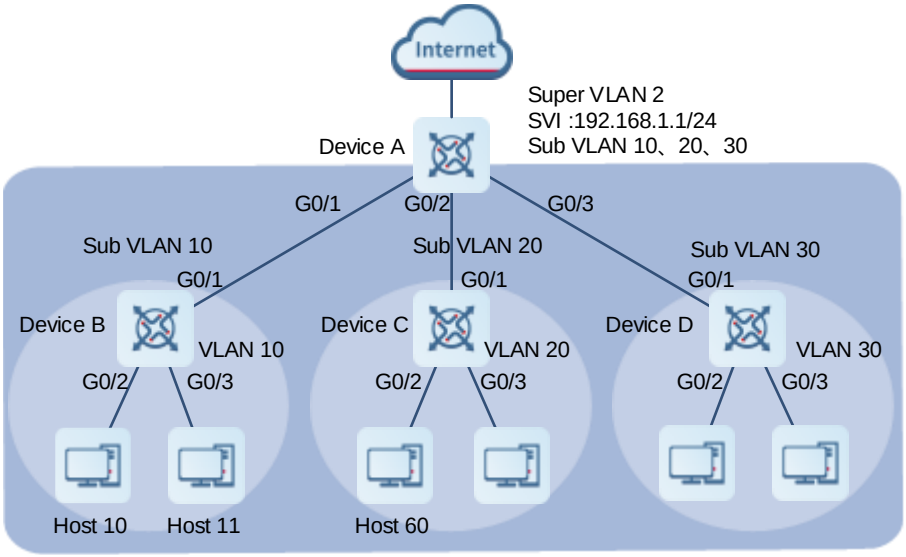
1. Requirements

A super VLAN 2 is configured and the network segment 192.168.1.0/24 is assigned to the super VLAN. Sub VLANs 10, 20 and 30 are added to the super VLAN. Hosts in the sub VLANs are in the same network segment and share a gateway IP address 192.168.1.1/24 to save IP addresses. Hosts are assigned static IP addresses. IP address ranges are configured for the three sub VLANs:

- Sub VLAN 10: 192.168.1.10/24 to 192.168.1.50/24
- Sub VLAN 20: 192.168.1.60/24 to 192.168.1.100/24
- Sub VLAN 30: 192.168.1.110/24 to 192.168.1.150/24

2. Topology

Figure 1-2 Application of Super VLAN



3. Notes

- Configure a super VLAN and sub VLANs on Device A (core device).
- Configure the common VLANs on Devices B, C, and D (access devices) that correspond to the sub VLANs on Device A.

4. Procedure

(1) Create a common VLAN to be configured as a sub VLAN.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan range 10,20,30
DeviceA(config-vlan-range)# exit
```

(2) Create VLAN 2, configure VLAN 2 as a super VLAN, configure VLANs 10, 20 and 30 as sub VLANs of the super VLAN, and configure VLAN 10 as a broadcast VLAN of the super VLAN.

```
DeviceA(config)# vlan 2
DeviceA(config-vlan)# supervlan
DeviceA(config-vlan)# subvlan 10,20,30
DeviceA(config-vlan)# bcast vlan 10
DeviceA(config-vlan)# exit
```

(3) Configure a gateway for the super VLAN.

```
DeviceA(config)# interface vlan 2
DeviceA(config-if-VLAN 2)# ip address 192.168.1.1 255.255.255.0
DeviceA(config-if-VLAN 2)# exit
```

(4) Configure IP address ranges for the sub VLANs.

```
DeviceA(config)# vlan 10
DeviceA(config-vlan)# subvlan-address-range 192.168.1.10 192.168.1.50
DeviceA(config-vlan)# exit
DeviceA(config)# vlan 20
DeviceA(config-vlan)# subvlan-address-range 192.168.1.60 192.168.1.100
DeviceA(config-vlan)# exit
DeviceA(config)# vlan 30
DeviceA(config-vlan)# subvlan-address-range 192.168.1.110 192.168.1.150
DeviceA(config-vlan)# exit
```

(5) Configure GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3 as trunk ports, and add them to the sub VLANs.

```
DeviceA(config)# interface range gigabitethernet 0/1,0/2,0/3
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode trunk
DeviceA(config-if-range)# end
DeviceA# write
```

5. Verification

(1) Check the super VLAN configuration.

```
DeviceA(config)# show supervlan
```

```
supervlan id  supervlan arp-proxy  bcast vlan  subvlan id  subvlan arp-proxy
subvlan ip range
------------  -------------------  ----------  ----------  -----------------
----------------
2           ON                10         10        ON   192.168.1.10 -
192.168.1.50
                                        20        ON   192.168.1.60 -
192.168.1.100
                                        30        ON   192.168.1.110 -
192.168.1.150
```

(2) Check ports that are added to VLANs.

```
DeviceA(config)# show vlan
VLAN      Name                          Status    Ports
---------- -------------------------------- ---------
-----------------------------------
        2 VLAN0002                      SUPER
       10 VLAN0010                      SUB      Gi0/1, Gi0/2, Gi0/3
       20 VLAN0020                      SUB      Gi0/1, Gi0/2, Gi0/3
       30 VLAN0030                      SUB      Gi0/1, Gi0/3, Gi0/3
```

(3) Verify that hosts in a sub VLAN can make L2 communication with each other.

On host 10 in sub VLAN 10, set the default gateway address to the gateway IP address of the super VLAN 192.168.1.1 and the IP address in the IP address range of the sub VLAN (that is, 192.168.1.10 to 192.168.1.50).

```
Host10> enable
Host10# configure terminal
Host10(config)# ip route 192.168.1.0 255.255.255.0 192.168.1.1
Host10(config)# interface gigabitethernet 0/1
Host10(config-if-GigabitEthernet 0/1)# no switchport
Host10(config-if-GigabitEthernet 0/1)# ip address 192.168.1.10 255.255.255.0
```

On host 11 in sub VLAN 10, set the default gateway address to the gateway IP address of the super VLAN 192.168.1.1 and the IP address in the IP address range of the sub VLAN (that is, 192.168.1.10 to 192.168.1.50).

```
Host11> enable
Host11# configure terminal
Host11(config)# ip route 192.168.1.0 255.255.255.0 192.168.1.1
Host11(config)#interface gigabitethernet 0/1
Host11(config-if-GigabitEthernet 0/1)# no switchport
Host11(config-if-GigabitEthernet 0/1)# ip address 192.168.1.11 255.255.255.0
```

Verify that host 10 can ping host 11 no matter whether the gateway IP address of the super VLAN is configured on Device A.

```
Host10# ping 192.168.1.11
Sending 5, 100-byte ICMP Echoes to 192.168.1.11, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms.
```

Set the IP address of host 11 to 192.168.1.51/24, which falls out of the IP address range of the sub VLAN, and verify that the communication of host 11 in the sub VLAN is not affected.

```
Host11(config-if-GigabitEthernet 0/1)# ip address 192.168.1.51 255.255.255.0
Host10# ping 192.168.1.51
Sending 5, 100-byte ICMP Echoes to 192.168.1.51, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/21/97 ms.
```

(4) Verify that hosts in different sub VLANs can make L3 communication but are isolated at L2.

On host 60 in sub VLAN 20, set the default gateway address to the gateway IP address of the super VLAN 192.168.1.1 and the IP address in the IP address range of the sub VLAN (that is, 192.168.1.60 to 192.168.1.100).

```
Host60> enable
Host60# configure terminal
Host60(config)# ip route 192.168.1.0 255.255.255.0 192.168.1.1
Host60(config)# interface gigabitethernet 0/1
Host60(config-if-GigabitEthernet 0/1)# no switchport
Host60(config-if-GigabitEthernet 0/1)# ip address 192.168.1.60 255.255.255.0
```

Configure an SVI and a gateway IP address for super VLAN 2, and verify that host 60 (192.168.1.60/24) can ping host 10 (192.168.1.10/24) and that host 60 cannot ping host 11 (192.168.1.51/24) because host 11 falls out of the IP address range of the sub VLAN.

```
Host60# ping 192.168.1.10
Sending 5, 100-byte ICMP Echoes to 192.168.1.10, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/19/95 ms.
Host60# ping 192.168.1.51
Sending 5, 100-byte ICMP Echoes to 192.168.1.51, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

Delete the gateway IP address of super VLAN 2, and verify that host 60 (192.168.1.60/24) cannot ping host 10 (192.168.1.10/24).

```
DeviceA(config)# interface vlan 2
DeviceA(config-if-VLAN 2)# no ip address
%notice: all IPv4 addresses on this interface are removed.
Host60# ping 192.168.1.10
Sending 5, 100-byte ICMP Echoes to 192.168.1.10, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

6. Configuration Files

- Device A configuration file

```
vlan 2
 supervlan
 subvlan 10,20,30
 bcast vlan 10
!
vlan 10
 subvlan-address-range 192.168.1.10 192.168.1.50
!
vlan 20
 subvlan-address-range 192.168.1.60 192.168.1.100
!
vlan 30
 subvlan-address-range 192.168.1.110 192.168.1.150
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface GigabitEthernet 0/3
 switchport mode trunk
!
interface VLAN 2
 ip address 192.168.1.1 255.255.255.0
```

- Device B configuration file

```
vlan range 1,10
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport access vlan 10
!
interface GigabitEthernet 0/3
 switchport access vlan 10
```

- Device C configuration file

```
vlan range 1,20
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
```

```
interface GigabitEthernet 0/2
 switchport access vlan 20
!
interface GigabitEthernet 0/3
 switchport access vlan 20
```

- Device D configuration file

```
vlan range 1,30
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport access vlan 30
!
interface GigabitEthernet 0/3
 switchport access vlan 30
```

7. Common Errors

- An SVI is configured for a common VLAN before the VLAN is configured as a sub VLAN. As a result, the common VLAN cannot be configured as a sub VLAN of a super VLAN.
- No SVI and gateway IP address are configured for a super VLAN. Consequently, communication between sub VLANs and between sub VLANs and other VLANs fails.
- Proxy ARP is disabled on the super VLAN or sub VLANs. Consequently, communication between the sub VLANs fails.
- An IP address range is configured for a sub VLAN. However, the static or dynamic IP addresses allocated to hosts in the sub VLAN are not in this range. Consequently, the hosts cannot make L3 communication.

Contents

1 Configuring Voice VLAN....1
1.1 Introduction....1
1.1.1 Overview....1
1.1.2 Background and Function....1
1.1.3 Identifying Voice Traffic....1
1.1.4 Work Mode of the Voice VLAN....2
1.1.5 Selection of the Work Mode....3
1.1.6 Security Mode of Voice VLAN....6
1.2 Configuration Task Summary....7
1.3 Configuring a Voice VLAN....7
1.3.1 Overview....7
1.3.2 Restrictions and Guidelines....7
1.3.3 Procedure....8
1.4 Configuring a Voice VLAN OUI....8
1.4.1 Overview....8
1.4.2 Restrictions and Guidelines....8
1.4.3 Procedure....8
1.5 Configuring a Voice Traffic Priority for a Voice VLAN....9
1.5.1 Overview....9
1.5.2 Restrictions and Guidelines....9
1.5.3 Prerequisites....9
1.5.4 Procedure....10

1.6 Configuration Aging Time for a Voice VLAN 10

1.6.1 Overview 10

1.6.2 Restrictions and Guidelines 10

1.6.3 Procedure 10

1.7 Configuring Security Mode for a Voice VLAN 11

1.7.1 Overview 11

1.7.2 Restrictions and Guidelines 11

1.7.3 Procedure 11

1.8 Configuring the Device to Automatically Add a Port to a Voice VLAN to Transmit Tagged Voice Traffic 11

1.8.1 Overview 11

1.8.2 Restrictions and Guidelines 11

1.8.3 Prerequisites 12

1.8.4 Procedure 12

1.9 Manually Adding a Port to a Voice VLAN to Transmit Tagged Voice Traffic 13

1.9.1 Overview 13

1.9.2 Restrictions and Guidelines 13

1.9.3 Prerequisites 13

1.9.4 Procedure 13

1.10 Manually Adding a Port to a Voice VLAN to Transmit Untagged Voice Traffic 14

1.10.1 Overview 14

1.10.2 Restrictions and Guidelines 14

1.10.3 Prerequisites 14

1.10.4 Procedure 15

1.11 Configuring LLDP to Deliver a Voice VLAN Policy 15

1.11.1 Overview 15

1.11.2 Restrictions and Guidelines 15

1.11.3 Prerequisites 16

1.11.4 Procedure 16

1.12 Monitoring 17

1.13 Configuration Examples 17

1.13.1 Configuring a Port to Transmit Tagged Voice Traffic in Automatic Mode 17

1.13.2 Configuring a Port to Transmit Untagged Voice Traffic in Manual Mode 21

1.13.3 Configuring Isolation of Untagged Voice Traffic from Data Traffic 23

1 Configuring Voice VLAN

1.1 Introduction

1.1.1 Overview

A voice virtual local area network (VLAN) is a VLAN dedicated to voice traffic of users. The voice VLAN technology constrains data traffic and voice traffic in the data VLAN and the voice VLAN, respectively, to prevent mutual interference between voice calls and data services and improve call quality.

1.1.2 Background and Function

- Background

Voice over IP (VoIP) telephones are widely used thanks to rapid development of technologies. Packet loss and latency greatly affect the quality of voice calls and users are more sensitive to the reduction of the quality of voice calls than the reduction of the quality of data or videos. Therefore, when the bandwidth is limited, it is necessary to guarantee the quality of voice data first so as to ensure the quality of voice calls.

- Functions of voice VLAN
  - a Identifies voice traffic.
  - b Supports automatic or manual adding of ports to a voice VLAN.
  - c Delivers Quality of Service (QoS) policies for voice traffic to improve the transmission priority of the voice traffic.
  - d Transmits voice data in a voice VLAN to ensure quality of voice calls.

1.1.3 Identifying Voice Traffic

Before assigning voice traffic to a voice VLAN, a switch device should be able to identify the voice traffic. Two methods can be used for the switch to identify voice data:

- Identifying voice data based on the Organizationally Unique Identifier (OUI) in the source MAC address of a packet

The source MAC address of a voice packet contains the OUI of a voice device vendor. After a voice VLAN OUI is configured, the device compares the source MAC address in a received packet with the voice VLAN OUI. If they match, the device can identify the voice packet and assign the packet to the voice VLAN.

Note

The MAC address field of an Ethernet packet is composed of 48 bits. The first 24 bits are referred to as an OUI, which is assigned by the Institute of Electrical and Electronics Engineers (IEEE) to device vendors. Each vendor assigns the last 24 bits based on this address segment to provide 48-bit MAC addresses.

- Identifying VoIP telephones based on the Link Layer Discovery Protocol (LLDP)

If there are a large number of VoIP telephones in a network, it is complex to configure OUIs of the VoIP telephones.

If a VoIP telephone supports LLDP, it automatically sends an LLDP packet when it goes online. This device can capture the LLDP packet and identify the device capability field in the packet. If the capability is "telephone", the device identifies the voice device as a VoIP telephone. Then, the device extracts the source MAC address from the packet and uses the address as the MAC address of the VoIP telephone, implementing automatic identification of the VoIP telephone.

If the policy of delivering a voice VLAN by LLDP is configured, this device can capture the LLDP packet from the VoIP telephone, fill voice VLAN information to related fields of the packet, and send the packet to the VoIP telephone. The VoIP telephone obtains the voice VLAN ID of this device. If the VoIP telephone supports tagged packets, it adds a VLAN tag to a voice packet before sending the packet. Upon receiving the tagged packet from the VoIP telephone, this device compares the VLAN tag in the packet with the voice VLAN ID. If they match, the device identifies the packet as a voice packet.

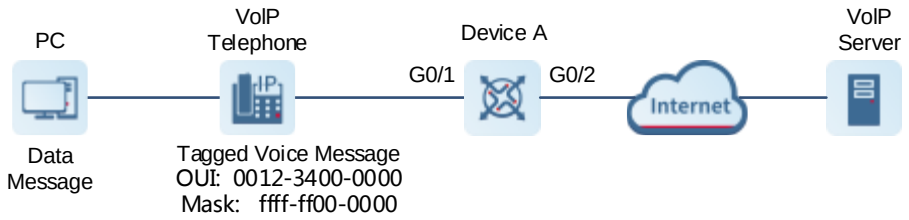
1.1.4 Work Mode of the Voice VLAN

The voice VLAN function supports manual and automatic work modes, which differ in the method of adding ports to a voice VLAN.

1. Automatic Mode

Connecting a PC and a VoIP telephone to a switch port in serial mode is the most common connection mode. The port transmits both voice data and common service data. When transmitting voice data, the port automatically forwards the voice packets to the voice VLAN. In this case, the port works in the automatic mode.

Figure 1-1 Network Topology of Voice VLAN in Automatic Mode



The working procedure of the voice VLAN in automatic mode is as follows:

(1) Adding a port to a voice VLAN: The device identifies the source MAC address in a packet, and compares the source MAC address with the OUI. If they match, the packet is identified as a voice packet. The voice packet can be identified based on a tag as well. The device automatically adds the input port of this voice packet to the voice VLAN and forwards the voice packet to the voice VLAN.

(2) Applying a priority policy: After the device identifies the voice packet based on the OUI, the device delivers a policy and changes the priority of the voice packet to the voice traffic priority.

(3) Removing the port from the voice VLAN after aging: The device maintains the port in the voice VLAN according to the aging mechanism. After the MAC address in the voice packet ages, if the port still fails to receive any voice packet within the aging time, the device removes this port from the voice VLAN.

Caution

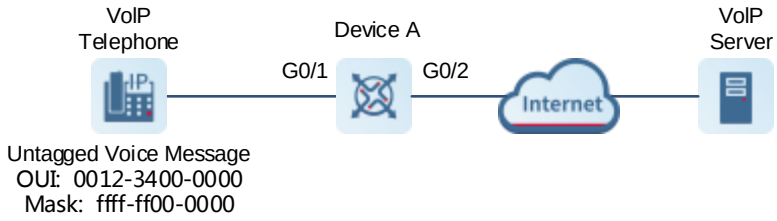
- In automatic mode, ports are automatically added to and removed from a voice VLAN. You are not allowed to manually add ports to a voice VLAN. Before you enable the voice VLAN function on a port, remove the voice VLAN from the allowed static VLAN list of the port to prevent the port from staying in the voice VLAN.

- Static MAC addresses do not age. Therefore, you are not advised to configure OUIs as static MAC addresses in automatic mode.

2. Manual Mode

If only a VoIP telephone is connected to a device port, the port transmits only voice packets. The administrator can manually add the port to a voice VLAN or remove the port from the voice VLAN. In this networking mode, the port transmits voice data only, which prevents service data from affecting transmission of voice data.

Figure 1-2 Network Topology of Voice VLAN in Manual Mode



The working procedure of the voice VLAN in manual mode is as follows:

(1) Applying a priority policy: The device identifies the source MAC address in a packet, and compares the source MAC address with the configured OUI. If they match, the device delivers a policy and changes the priority of the voice packet to the voice traffic priority.

1.1.5 Selection of the Work Mode

You can find out whether voice traffic contains tags based on the type and configuration of VoIP telephones and then select a proper work mode for the device.

1. Types of VoIP Telephones

Like any other network device, a VoIP telephone needs an IP address before it can implement communication normally in the network. VoIP telephones are categorized into two types, based on whether they automatically obtain IP addresses and voice VLAN information. One type of VoIP telephones can automatically obtain IP addresses and voice VLAN IDs. The other type of VoIP telephone requires you to configure IP addresses and voice VLAN IDs for them. The two types of VoIP telephones may send tagged and untagged voice traffic.

- VoIP telephones that can automatically obtain IP addresses and voice VLAN IDs

  The VoIP telephones can automatically obtain IP addresses via the Dynamic Host Configuration Protocol (DHCP).

  A VoIP telephone requests voice VLAN information from the DHCP server. If the DHCP server returns the required information, the VoIP telephone sends a voice packet carrying the voice VLAN tag. If the DHCP server does not return the required information, the VoIP telephone sends a voice packet that does not carry the voice VLAN tag.

- VoIP telephones in need of manual configuration of IP addresses and voice VLAN IDs

  IP addresses must be manually configured. Otherwise, the VoIP telephones cannot normally work.

If a voice VLAN ID is configured for a VoIP telephone, the VoIP telephone sends and receives only tagged voice traffic based on the configuration. If no voice VLAN ID is configured for a VoIP telephone, the VoIP telephone sends and receives only untagged voice traffic.

2. Types of Voice Traffic

- Tagged voice traffic

  When a VoIP telephone obtains voice VLAN information automatically or via manual configuration, the VoIP telephone sends tagged voice traffic.

  In this case, a port can be configured as a trunk, hybrid, or uplink port. The port sends data packets to the native VLAN, and sends tagged voice packets to a non-native VLAN that is used as a voice VLAN. A voice VLAN supports both automatic and manual modes.

  - In automatic mode, the allowed static VLAN list of a port must contain the native VLAN and exclude the voice VLAN, and the voice VLAN is automatically added to or removed from the allowed VLAN list of the port. After the voice VLAN function is enabled on the port, when the port receives a tagged voice packet, the port is added to the voice VLAN to transmit tagged voice traffic. If the port does not receive a new voice packet within the aging time after the MAC address in the packet ages, the port removes the voice VLAN from the allowed VLAN list of the port.
  - In manual mode, the native VLAN and voice VLAN must be added to the allowed static VLAN list of a port.

- Untagged voice traffic

  If a VoIP telephone automatically obtains an IP address but does not obtain voice VLAN information, or an IP address is configured for the VoIP telephone but no voice VLAN is configured, the VoIP telephone sends and receives untagged voice traffic.

  In this case, the voice VLAN of the port must work in manual mode. You must configure a native VLAN for the receive port and allow packets with the native VLAN ID to pass. The native VLAN can be configured as a voice VLAN so that untagged voice packets are transmitted over the voice VLAN.

Note

VoIP telephones from different vendors may be different in the work principle, support for voice VLAN, and the process of obtaining IP addresses and voice VLAN information. For more information, see the user manual of the VoIP telephone.

3. Supported Work Modes

Table 1-1 Work Modes for Tagged Voice Traffic

Mode	Port Type	Supported Work Mode and Configuration Requirement
Automatic mode	Trunk Hybrid Uplink	Automatic mode is supported. Configuration requirements: The native VLAN is added to the allowed VLAN list of a port to transmit common data. The voice VLAN is removed from the allowed VLAN list of the port and the port can join or exit the VLAN automatically. A native VLAN cannot be configured as a voice VLAN.

Mode	Port Type	Supported Work Mode and Configuration Requirement
	Access Promiscuous Host	The access ports, promiscuous ports of PVLAN, and host ports do not support tagged voice traffic.
Manual mode	Trunk Hybrid Uplink	Manual mode is supported. Configuration requirements: Both the native VLAN and voice VLAN (tagged) are added to the allowed VLAN list of a port. A native VLAN cannot be configured as a voice VLAN.
	Access Promiscuous Host	The access ports, promiscuous ports of PVLAN, and host ports do not support tagged voice traffic.

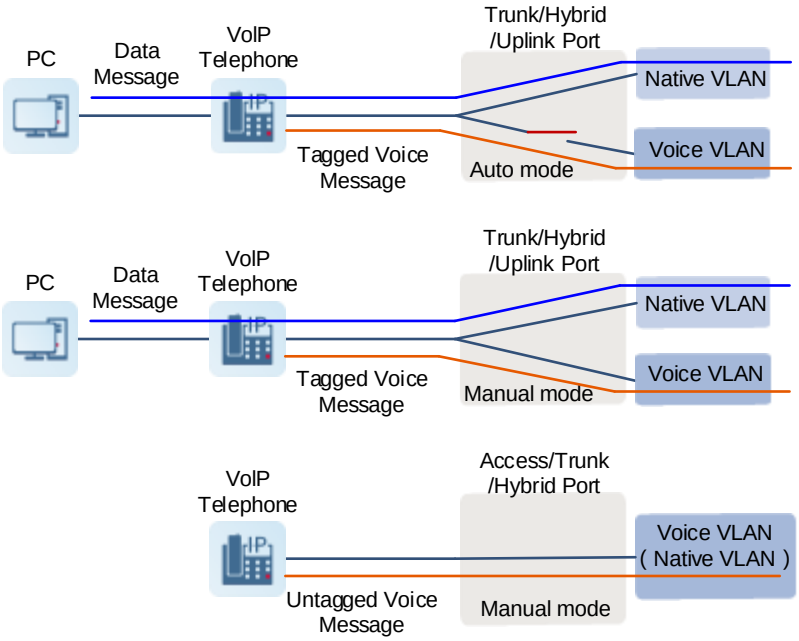
Table 1-2 Work Modes for Untagged Voice Traffic

If the voice traffic is untagged, the device supports only the manual mode.

Mode	Port Type	Supported Work Mode and Configuration Requirement
Manual mode	Access	Manual mode is supported. Configuration requirement: The voice VLAN is the VLAN, to which the access port belongs.
	Host	Manual mode is supported. Configuration requirement: The voice VLAN is the secondary VLAN (isolated or community VLAN) of a host port.
	Promiscuous	Manual mode is supported. Configuration requirement: A voice VLAN is the primary VLAN of a promiscuous port.
	Trunk	Manual mode is supported. Configuration requirement: The voice VLAN is the native VLAN of an access port and the port allows packets with the native VLAN ID to pass.
	Hybrid	Manual mode is supported. Select either of the following configuration methods: ● The voice VLAN is the native VLAN of an access port and the port allows packets with the native VLAN ID to pass through. ● The MAC VLAN function is configured to identify packets with MAC addresses matching the MAC address of a VoIP telephone as voice traffic and assign them to the voice VLAN. In this case, the voice VLAN is not necessarily configured as a native VLAN of a hybrid port.
	Uplink	When the voice traffic is untagged, the port cannot be configured as an

Mode	Port Type	Supported Work Mode and Configuration Requirement
		uplink port (not sending untagged packets).

Figure 1-3 Work Mode Selection



1.1.6 Security Mode of Voice VLAN

When a port is added to a voice VLAN, the device no longer checks the source MAC address in the packets. Theoretically, all voice packets can be transmitted over the voice VLAN. Therefore, the device may suffer malicious packet attacks, which affects normal voice communication in the voice VLAN.

To better isolate voice traffic from data traffic during transmission, the device provides the security mode for a voice VLAN.

When the security mode is enabled, only voice traffic can be transmitted in the voice VLAN. The device checks the source MAC address in each packet. When the source MAC address in the packet matches the voice VLAN OUI, the packet can be transmitted in the voice VLAN. Otherwise, the device discards the packet.

Note

In security mode, the device checks the source MAC addresses of only untagged packets and tagged packets with the voice VLAN ID. For tagged packets with non-voice VLAN IDs, the device forwards or discards the packets according to VLAN rules, irrespective of the security/common mode of the voice VLAN.

Caution

It is not recommended that both voice data and service data be transmitted over the voice VLAN. If you want to transmit both voice data and service data over the voice VLAN, disable the voice VLAN function in security mode.

1.2 Configuration Task Summary

Configuring Voice VLAN The configuration includes the following tasks:

(1) Configuring a Voice VLAN

(2) (Optional) Configuring a Voice VLAN OUI

(3) (Optional) Configuring a Voice Traffic Priority for a Voice VLAN

(4) (Optional) Configuration Aging Time for a Voice VLAN

(5) (Optional) Configuring Security Mode for a Voice VLAN

(6) Add a port to a voice VLAN and enable the voice VLAN function on the port. Select at least one of the following to configure.

- Configuring the Device to Automatically Add a Port to a Voice VLAN to Transmit Tagged Voice Traffic
- Manually Adding a Port to a Voice VLAN to Transmit Tagged Voice Traffic
- Manually Adding a Port to a Voice VLAN to Transmit Untagged Voice Traffic

(7) (Optional) Configuring LLDP to Deliver a Voice VLAN Policy

1.3 Configuring a Voice VLAN

1.3.1 Overview

You can create a voice VLAN on a device used to transmit voice packets only, and enable the voice VLAN function in global configuration mode. The voice VLAN function must be enabled on the port that is connected to a VoIP telephone so that the voice VLAN function can take effect.

1.3.2 Restrictions and Guidelines

- Only one voice VLAN can be configured. You must disable the voice VLAN function before you modify the voice VLAN ID. You can use the **no voice vlan** command to disable the voice VLAN function in global configuration mode.
- You must create a VLAN before configuring a voice VLAN. VLAN IDs must meet the following requirements:
  - VLAN 1 cannot be configured as a voice VLAN. Therefore, the value range of *vlanid* is from 2 to 4094.
  - A VLAN cannot be configured as a voice VLAN and a super VLAN at the same time.
  - A protocol VLAN is valid to only untagged packets received by a trunk or hybrid port. In a voice VLAN in automatic mode, the trunk and hybrid ports can process only tagged voice traffic. Therefore, do not configure a VLAN as a protocol VLAN and a voice VLAN at the same time.
  - If the 802.1x automatic VLAN hopping function is enabled on an access port, do not configure the VLAN ID delivered by 802.1x as the voice VLAN ID to ensure that the function works properly.
  - If a VoIP telephone sends tagged voice traffic and the 802.1x authentication and guest VLAN functions are enabled on the access port, configure different VLAN IDs for the voice VLAN, native VLAN, and 802.1x guest VLAN to ensure proper running of the functions.
  - Do not configure a VLAN as a remote VLAN of the remote switched port analyzer (RSPAN) and a voice VLAN at the same time. Otherwise, the RSPAN and voice VLAN functions may be affected.

- If a PC and a VoIP telephone are connected to the same port in serial mode, and both the 802.1x authentication and voice VLAN functions are enabled on the port, the PC must pass 802.1X authentication to access the network. If the OUI of the VoIP telephone matches the voice VLAN OUI, the VoIP telephone can make communication via the voice VLAN without passing 802.1x authentication.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a VLAN.

vlan *voice-vlan-id*

Only VLAN 1 exists by default.

(4) Return to the global configuration mode.

exit

(5) Configure the VLAN as a voice VLAN.

voice vlan *voice-vlan-id*

No voice VLAN is configured by default.

1.4 Configuring a Voice VLAN OUI

1.4.1 Overview

After a VoIP telephone is connected to the device, you must configure the OUI of the VoIP telephone on the device so that the VoIP telephone can communicate over the network.

The device allows you to set an OUI to be identified by the voice VLAN function. For more information about the OUI, see the principle of the voice VLAN function. The device that supports the voice VLAN function identifies the source MAC address in a received packet, and compares the source MAC address with the OUI of the voice VLAN configured on the device to check whether the traffic is sent from a specified voice device. The priority of a received packet can be changed to the voice traffic priority only when the source MAC address in the packet matches the OUI of the voice VLAN.

1.4.2 Restrictions and Guidelines

- The OUI of the voice VLAN cannot be a multicast address, and the configured mask should not contain non-consecutive 1's.
- *mac-address* indicates the source MAC address in a voice packet. *oui-mask* indicates the valid length of an OUI, which is expressed by a mask. *text* indicates a descriptor of an OUI.
- You can use the **no voice vlan mac-address oui** command in global configuration mode to delete an OUI configured on a device.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a voice VLAN OUI.

voice vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

No OUI is configured by default.

1.5 Configuring a Voice Traffic Priority for a Voice VLAN

1.5.1 Overview

You can modify the Class of Service (CoS) and differentiated services code point (DSCP) values for voice traffic in a voice VLAN on the device to improve the priority of the voice traffic and the quality of voice calls.

- The CoS value indicates L2 priority and is represented by three bits. The value range is from 0 to 7. A larger value indicates a higher priority. The CoS value is stored in the L2 header of a packet and filled in the PRI field of an 802.1Q VLAN tag. The CoS value of a common VLAN packet is **0**, which indicates the lowest priority. The default CoS value of voice traffic in a voice VLAN is **6**, which indicates a higher priority than common VLAN packets.
- The DSCP value indicates IP priority (IP PRE) and is represented by six bits. The value range is from 0 to 63. A larger value indicates a higher priority. The DSCP value is stored in the L3 header of a packet. For an IPv4 packet, the DSCP value is filled in the first six bits (bit 0 to bit 5) of the type of service (ToS) field in the header of the packet. For an IPv6 packet, the DSCP value is filled in the first six bits in the **Traffic Class** field of the IPv6 packet header. The DSCP value of a common IP packet is **0**, which indicates the lowest priority. The default DSCP value of voice traffic in a voice VLAN is **46**, which indicates a higher priority than common IP packets.
- The packet trust mode of the QoS module is disabled by default. This causes the QoS module to change the priority of all packets to **0**, and overwrites the packet priority modified by the voice VLAN function. You must run the **mls qos trust** { **cos** | **ip-precedence** | **dscp** | **exp** } command in interface configuration mode, and select the **cos** and **dscp** parameters to enable the trust mode of the QoS module to trust the packet priority modified by the voice VLAN function.

For more information about CoS and DSCP, see *Configuring CoS*.

1.5.2 Restrictions and Guidelines

- To restore the QoS and DSCP values to default values, you can run the **no voice vlan cos** or **no voice vlan dscp** command in global configuration mode.
- *cos-value* indicates the CoS value of voice traffic in a voice VLAN. The value range is from 0 to 7, and the default value is **6**.
- *dscp-value* indicates the DSCP value of voice traffic in a voice VLAN. The value range is from 0 to 63, and the default value is **46**.

1.5.3 Prerequisites

A voice VLAN has been configured. A OUI has been configured.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(1) Enter the global configuration mode.

configure terminal

(2) Specify the priority of voice packets in a voice VLAN.

voice vlan { **cos** *cos-value* | **dscp** *dscp-value* }

The default CoS and DSCP values of voice packets are **6** and **46**, respectively.

(3) Enter the interface configuration mode of the port connected to a voice device.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

(4) Enable the trust mode of the QoS module to trust the priority of voice packets.

mls qos trust { **cos** | **dscp** }

The trust mode of the QoS module is disabled by default.

1.6 Configuration Aging Time for a Voice VLAN

1.6.1 Overview

In automatic mode, after the MAC address in a voice packet ages, if the port does not receive any more voice packets within the aging time, the device removes this port from the voice VLAN.

The aging time is only valid in automatic mode. In manual mode, the aging time is invalid and therefore does not need to be configured.

1.6.2 Restrictions and Guidelines

- The aging time of a voice VLAN starts after the MAC address in a voice packet ages. The value range is from 5 to 10000, in minutes.
- To restore the aging time to the default value, you can run the **no voice vlan aging** command in global configuration mode.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure aging time of a voice VLAN.

voice vlan aging *age*

The default aging time of a voice VLAN is 1440 minutes.

1.7 Configuring Security Mode for a Voice VLAN

1.7.1 Overview

To guarantee quality of voice traffic during transmission and prevent malicious attacks, you can enable the security mode of a voice VLAN to allow only voice traffic to be transmitted in the voice VLAN.

1.7.2 Restrictions and Guidelines

To disable the security mode of the voice VLAN, you can run the **no voice vlan security enable** command in global configuration mode.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the security mode of the voice VLAN.

voice vlan security enable

The security mode of a voice VLAN is enabled by default.

1.8 Configuring the Device to Automatically Add a Port to a Voice VLAN to Transmit Tagged Voice Traffic

1.8.1 Overview

To use a port for VoIP telephone communication, you must add the port to a voice VLAN, configure the work mode for the voice VLAN, and enable the voice VLAN function on the port.

1.8.2 Restrictions and Guidelines

- You can enable the voice VLAN function only on an L2 physical port (for example, access, trunk, hybrid, uplink, or private VLAN port). The function cannot be enabled on an aggregation port or a routing port.
- Even if the voice VLAN function is disabled in global configuration mode, you can still enable the voice VLAN function on a port but the configuration does not take effect.
- When a port works in automatic mode, the native VLAN is used to transmit common VLAN packets. Do not configure the native VLAN of the port as a voice VLAN. If a port is automatically added to a voice VLAN after the port identifies voice traffic, you cannot manually add the port to or delete the port from the voice VLAN by using commands.
- If a port does not transmit packet data of a voice VLAN, remove the voice VLAN from the allowed VLAN list of the port.
- When a port works in manual mode, you must manually add the port to the voice VLAN to ensure that the voice VLAN function can take effect. To configure a port to work in manual mode, you can run the **no voice vlan mode auto** command.
- After the voice VLAN function is enabled on a port, you are not allowed to switch the port between the

manual mode and automatic mode and the allowed VLAN list of the port cannot be changed. To change the voice VLAN work mode or the allowed VLAN list of the port, disable the voice VLAN function on the port first. After the voice VLAN function is enabled on a port, to ensure normal operation of the function, you are not advised to change the port type (such as access, trunk, or hybrid port). To change the port type, disable the voice VLAN function on this port first. To disable the voice VLAN function of a port, you can run the **no voice vlan enable** command.

- If the voice traffic is tagged, a user port can be configured as a trunk, hybrid, or uplink port. The access port, host port of PVLAN, and promiscuous port of PVLAN do not support tagged voice traffic.
- If you want to transmit untagged common packets from a PC and tagged voice packets from a VoIP telephone over a user port, configure the user port as a trunk port and configure the device to automatically add the port to a voice VLAN. The configuration steps are as follows: The configuration steps for a hybrid or an uplink port are similar to the following configuration steps.

1.8.3 Prerequisites

Configure a voice VLAN.

1.8.4 Procedure

(1) Create a data VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a VLAN to transmit common packets.

vlan *data-vlan-id*

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the native VLAN of a user port as a data VLAN, add the data VLAN to the allowed VLAN list of the port, and exclude the voice VLAN from the allowed VLAN list.

a Enter the interface configuration mode.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

b Configure the user port as a trunk port.

switchport mode trunk

An interface works in access mode by default.

c Configure the VLAN used for transmitting common packets as a native VLAN of the user port to transmit untagged common packets.

switchport trunk native vlan *data-vlan-id*

The default native VLAN of a trunk port is VLAN 1.

d Configure an allowed VLAN list for the user port, add the data VLAN to the list, and exclude the voice VLAN from the list.

switchport trunk allowed vlan remove *voice-vlan-id*

The default allowed VLANs of a trunk port are VLANs 1 to 4094.

(3) Configure the voice VLAN to work in automatic mode so that the voice VLAN is automatically added to the allowed VLAN list of this port when the port receives voice data.

voice vlan mode auto

A voice VLAN works in automatic mode by default.

(4) Enable the voice VLAN function on the user port.

voice vlan enable

The voice VLAN function is disabled on a port by default.

1.9 Manually Adding a Port to a Voice VLAN to Transmit Tagged Voice Traffic

1.9.1 Overview

To use a port for VoIP telephone communication, you must add the port to a voice VLAN, configure the work mode for the voice VLAN, and enable the voice VLAN function on the port.

1.9.2 Restrictions and Guidelines

- If the voice traffic is tagged, a user port can be configured as a trunk, hybrid, or uplink port. The access port, host port of PVLAN, and promiscuous port of PVLAN do not support tagged voice traffic. Therefore, they cannot be added to a voice VLAN.
- If you want to transmit untagged common packets from a PC and tagged voice packets from a VoIP telephone over a user port, configure the user port as a trunk port and manually add the port to a voice VLAN. The configuration steps are as follows: The configuration steps for a hybrid or an uplink port are similar to the following configuration steps.

1.9.3 Prerequisites

Configure a voice VLAN.

1.9.4 Procedure

(1) Create a data VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a VLAN to transmit common packets.

vlan *data-vlan-id*

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the native VLAN of the user port as a data VLAN, and add the data VLAN and voice VLAN to the allowed VLAN list of the port.

a Enter the interface configuration mode.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

b Configure the user port as a trunk port.

switchport mode trunk

An interface works in access mode by default.

c Configure the VLAN used for transmitting common packets as a native VLAN of the user port to transmit untagged common packets.

switchport trunk native vlan *data-vlan-id*

The default native VLAN of a trunk port is VLAN 1.

d Configure an allowed VLAN list for the user port, and add only the data VLAN and voice VLAN to the allowed VLAN list.

switchport trunk allowed vlan only *data-vlan-id*,*voice-vlan-id*

The default allowed VLANs of a trunk port are VLANs 1 to 4094.

(3) Configure the voice VLAN to work in manual mode.

no voice vlan mode auto

A voice VLAN works in automatic mode by default.

(4) Enable the voice VLAN function on the user port.

voice vlan enable

The voice VLAN function is disabled on a port by default.

1.10 Manually Adding a Port to a Voice VLAN to Transmit Untagged Voice Traffic

1.10.1 Overview

To use a port for VoIP telephone communication, you must add the port to a voice VLAN, configure the work mode for the voice VLAN, and enable the voice VLAN function on the port.

1.10.2 Restrictions and Guidelines

- When the voice traffic is untagged, you must manually add a port to a voice VLAN. The port type can be access port, trunk port, hybrid port, host port of PVLAN, or promiscuous port of PVLAN. The uplink port does not send untagged packets. Therefore, it cannot be added to a voice VLAN.
- If you want to transmit untagged voice packets from a VoIP telephone over a user port, configure the user port as an access port and manually add the port to a voice VLAN. The configuration steps are as follows:

1.10.3 Prerequisites

Configure a voice VLAN.

1.10.4 Procedure

(1) Add a user port to a voice VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Enter the interface configuration mode.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

d Configure the user port as an access port.

switchport mode access

An interface works in access mode by default.

e Add the access port to the voice VLAN to transmit common untagged packets.

switchport access vlan *voice-vlan-id*

An access port belongs to VLAN 1 by default.

(2) Configure the voice VLAN to work in manual mode.

no voice vlan mode auto

A voice VLAN works in automatic mode by default.

(3) Enable the voice VLAN function on the user port.

voice vlan enable

The voice VLAN function is disabled on a port by default.

1.11 Configuring LLDP to Deliver a Voice VLAN Policy

1.11.1 Overview

A VoIP telephone supporting the LLDP function automatically sends an LLDP packet when it goes online. If the LLDP Network Policy type/length/value (TLV) function is enabled on this device, the device can capture the LLDP packet sent by the VoIP telephone and deliver a voice VLAN policy to the VoIP telephone. If a voice VLAN policy requires the VoIP telephone to send tagged frames and the VoIP telephone supports tagged frames, the VoIP telephone adds a VLAN tag to voice packets before transmission according to the voice VLAN policy. If the voice VLAN policy requires the VoIP telephone to send untagged frames, the VoIP telephone sends untagged packets.

If the VoIP telephone does not support the Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED), you must manually add the MAC address of the VoIP telephone to the OUI list of the voice VLAN.

1.11.2 Restrictions and Guidelines

- You can run the **lldp network-policy profile** *profile-num* command in global configuration mode to create a policy or enter the LLDP network policy configuration mode of a policy. *profile-num* indicates the ID of an LLDP network policy. The value range is from 1 to 1024.
- After entering the LLDP network policy configuration mode, you can run the { **voice** | **voice-signaling** } **vlan**

command to configure a specific network policy. You can run the **no** { **voice** | **voice-signaling** } **vlan** command to delete a voice VLAN policy.

- You can run the **no lldp network-policy profile** *profile-num* command in interface configuration mode to delete an LLDP network policy.
- For more information about command description, see *Configuring LLDP*.

1.11.3 Prerequisites

- A voice VLAN has been configured.
- The trust mode of the QoS module has been enabled to trust packet priority modification.
- The port connected to a VoIP telephone has been manually added to a voice VLAN and the voice VLAN function has been enabled on the port.
  - To enable the VoIP telephone to send tagged frames, see Manually Adding a Port to a Voice VLAN to Transmit Tagged Voice Traffic.
  - To enable the VoIP telephone to send untagged voice traffic, see Manually Adding a Port to a Voice VLAN to Transmit Untagged Voice Traffic.

1.11.4 Procedure

(1) Create an LLDP network policy and enter the configuration mode.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create an LLDP network policy and enter the LLDP network policy configuration mode.

lldp network-policy profile *profile-num*

No LLDP network policy is configured by default.

(2) Configure a voice VLAN policy. Select at least one of the following to configure:

- Configure a policy to enable the VoIP telephone to send tagged frames, with the VLAN ID of *voice-vlan-id* or **0** and priority of *cos* and *dscp*.

  { **voice** | **voice-signaling** } **vlan** { *voice-vlan-id* | **dot1p** } [**cos** *cos* | **dscp** *dscp*]

  The default CoS value and DSCP value of voice packets in a voice VLAN are **6** and **46** respectively.

- Configure a policy to enable the VoIP telephone to send untagged frames. In this case, you need to manually add the port to the voice VLAN.

  { **voice** | **voice-signaling** } **vlan untagged**

  No voice VLAN policy is configured by default.

(3) Configure the user port to allow advertising the Network Policy TLV.

a Return to the global configuration mode.

exit

b Enter the interface configuration mode.

interface *interface-type interface-number*

c Configure the port to allow advertising the Network Policy TLV.

lldp tlv-enable med-tlv network-policy profile *profile-num*

No port is allowed to advertise the Network Policy TLV by default.

1.12 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

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

Run the **clear** commands to clear information.

Caution

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

Table 1-3 Monitoring

Command	Purpose
show voice vlan	Displays the voice VLAN configuration.
show voice vlan oui	Displays the OUI configuration of the voice VLAN.
debug bridge vvlan	Debugs the voice VLAN function.

1.13 Configuration Examples

1.13.1 Configuring a Port to Transmit Tagged Voice Traffic in Automatic Mode

1. Requirements

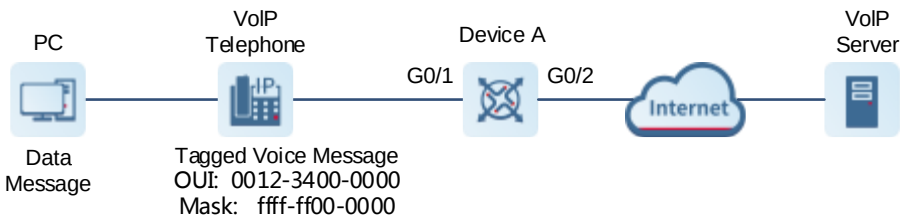
Each office staff member is assigned an Ethernet port. This port is used for service communication of a PC and voice communication of a VoIP telephone.

The VoIP telephone can automatically obtain an IP address and voice VLAN information and send tagged voice traffic. The MAC address of the VoIP telephone is 0012.3456.7890 and the OUI is 0012.3400.0000. To ensure the quality of voice calls, voice traffic is directed to a voice VLAN. The port aging time is set to 1000 minutes, CoS value to **5**, and DSCP value to **40**. The security mode of the voice VLAN needs to be enabled to transmit only voice traffic.

The PC is connected to the network through the VoIP telephone in serial mode and the PC sends untagged data traffic. The data traffic of the PC is isolated from the voice traffic of the VoIP telephone.

2. Topology

Figure 1-4 Network Topology of Voice VLAN in Automatic Mode



3. Notes

- The link needs to carry both tagged voice traffic and untagged data traffic. Therefore, set the port connected to the VoIP telephone to work in automatic mode.
- Configure GigabitEthernet 0/1 as a trunk port so that data traffic is transmitted in native VLAN 5 and voice traffic is transmitted in voice VLAN 2 separately.
- In automatic mode, GigabitEthernet 0/1 is automatically added to the voice VLAN. You are not allowed to manually add the port to the voice VLAN. Remove voice VLAN 2 from the allowed VLAN list of GigabitEthernet 0/1 so that the port determines whether to reside in the voice VLAN based on the aging time. The aging time must be configured for the port.
- GigabitEthernet 0/1 is connected to the VoIP telephone that automatically obtains an IP address. After the VoIP telephone obtains an IP address in the voice VLAN, the VoIP telephone can be normally used.
- (Optional) If 802.1x authentication is needed for the PC, enable the 802.1x authentication function on GigabitEthernet 0/1; to enable the voice packets of the VoIP telephone to be forwarded to the voice VLAN without 802.1x authentication, configure a security channel and an ACL policy. For more information about the support of this function and specific configuration, see the *Configuring 802.1X* and *Configuring ACL*.

4. Procedure

(1) Configure voice VLAN 2 to transmit voice traffic.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan 2
DeviceA(config-vlan)# exit
DeviceA(config)# voice vlan 2
```

(2) Set the OUI used for identifying voice packets to 0012.3400.0000, mask to ffff.ff00.0000, and vendor to B. The priority of a received packet can be changed only when the source MAC address in the packet matches the voice VLAN OUI.

```
DeviceA(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description B
```

(3) Set the CoS value to **5** and the DSCP value to **40** for voice traffic of the voice VLAN.

```
DeviceA(config)# voice vlan cos 5
DeviceA(config)# voice vlan dscp 40
```

(4) Set the aging time of the voice VLAN to 1000 minutes. This configuration is required in automatic mode only.

```
DeviceA(config)# voice vlan aging 1000
```

(5) Enable the security mode of the voice VLAN. This mode is enabled by default.

```
DeviceA(config)# voice vlan security enable
```

(6) Create VLAN 5 to transmit common data.

```
DeviceA(config)# vlan 5
DeviceA(config-vlan)# exit
```

(7) Configure GigabitEthernet 0/1 as a trunk port and data VLAN 5 as a native VLAN of the port, and remove voice VLAN 2 from the allowed VLAN list of GigabitEthernet 0/1 so that voice VLAN 2 is automatically added to the allowed VLAN list of the port.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/1)# switchport trunk native vlan 5
DeviceA(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan remove 2
```

(8) Enable the trust mode of the QoS module to trust the packet priority modification. Configure automatic adding of the port to the voice VLAN and enable the voice VLAN function on the port. The voice VLAN works in automatic mode by default.

```
DeviceA(config-if-GigabitEthernet 0/1)# mls qos trust cos
DeviceA(config-if-GigabitEthernet 0/1)# voice vlan mode auto
DeviceA(config-if-GigabitEthernet 0/1)# voice vlan enable
```

(9) (Optional) Enable 802.1x authentication on GigabitEthernet 0/1. Configure a security channel and an ACL policy.

```
DeviceA(config-if-GigabitEthernet 0/1)# dot1x port-control auto
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# expert access-list extended safe_channel
DeviceA(config-exp-nacl)# permit etype-any 0012.3400.0000 0000.00ff.ffff any
DeviceA(config-exp-nacl)# exit
DeviceA(config)# security global access-group safe_channel
```

(10) Configure the uplink port GigabitEthernet 0/2 as a trunk port.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/2)# end
DeviceA# write
```

5. Verification

Run the **show voice vlan** command to check the current status of the voice VLAN on the device.

```
DeviceA# show voice vlan
Voice Vlan status: ENABLE
Voice Vlan ID       : 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1000 minutes
Voice Vlan cos      : 5
Voice Vlan dscp     : 40
Current voice vlan enabled port mode:
```

```
PORT                MODE
-------------------- ----------
Gi0/1               AUTO
```

Check the voice VLAN OUI of the device.

```
DeviceA# show voice vlan oui
Oui           Mask            Description
0012.3400.0000  ffff.ff00.0000   B
```

Check port configuration.

```
DeviceA# show interface swithport
Interface           Switchport Mode     Access Native Protected VLAN lists
--------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1   enabled   TRUNK    1     5     Disabled  1,3-4094
GigabitEthernet 0/2   enabled   TRUNK    1     1     Disabled  ALL
```

6. Configuration Files

Device A configuration file

```
voice vlan 2
voice vlan cos 5
voice vlan dscp 40
voice vlan aging 1000
voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description "B"
!
expert access-list extended safe_channel
 10 permit etype-any 0012.3400.0000 0000.00ff.ffff any
!
security global access-group safe_channel
!
vlan range 1-2,5
!
interface GigabitEthernet 0/1
 switchport mode trunk
 switchport trunk native vlan 5
 switchport trunk allowed vlan only 1,3-4094
 voice vlan enable
 dot1x port-control auto
 mls qos trust cos
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

7. Common Errors

- When a voice VLAN works in automatic mode, the voice VLAN is not removed from the allowed VLAN list of the port.
- The trust mode of the QoS module is not enabled. Consequently, the packet priority modification cannot take

effect, affecting voice traffic transmission.

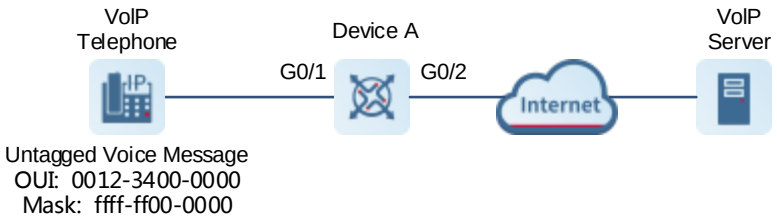
1.13.2 Configuring a Port to Transmit Untagged Voice Traffic in Manual Mode

1. Requirements

A VoIP telephone is connected to voice VLAN 2 through GigabitEthernet 0/1 of device A. This link carries only voice traffic. This type of networking is generally used when VoIP telephones are deployed in conference rooms or when no PC is required to transmit data services. The port connected to the VoIP telephone is set to work in manual mode to send untagged voice traffic to device A. The security mode is enabled to enable the voice VLAN to transmit only voice traffic. The CoS value is changed to **5** and the DSCP value is changed to **40** for the voice VLAN.

2. Topology

Figure 1-5 Network Topology of Voice VLAN in Manual Mode



3. Notes

- GigabitEthernet 0/1 receives only untagged voice traffic from the VoIP telephone. Since the untagged voice traffic cannot be forwarded in automatic mode. Therefore, configure the voice VLAN on the port to work in manual mode.
- You can configure GigabitEthernet 0/1 as a hybrid port and voice VLAN 2 as a native VLAN, and add the voice VLAN to the allowed untagged VLAN list of the port. You can also configure GigabitEthernet 0/1 as an access port, and add the port to the voice VLAN. In the following example, GigabitEthernet 0/1 is configured as an access port.

4. Procedure

(1) Create VLAN 2, and configure this VLAN as a voice VLAN.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan 2
DeviceA(config-vlan)# exit
DeviceA(config)# voice vlan 2
```

(2) Set the CoS value to **5** and the DSCP value to **40** for voice traffic of the voice VLAN.

```
DeviceA(config)# voice vlan cos 5
DeviceA(config)# voice vlan dscp 40
```

(3) Set the OUI for identifying voice packets to 0012.3400.0000, mask to ffff.ff00.0000, and vendor to B on the device.

```
DeviceA(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description B
```

(4) Enable the security mode of the voice VLAN. This mode is enabled by default.

```
DeviceA(config)# voice vlan security enable
```

(5) Configure GigabitEthernet 0/1 as an access port and add the port to voice VLAN 2.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode access
DeviceA(config-if-GigabitEthernet 0/1)# switchport access vlan 2
```

(6) Enable the trust mode of the QoS module to trust the priority of voice packets. Manually add the user port to the voice VLAN and enable the voice VLAN function on the port.

```
DeviceA(config-if-GigabitEthernet 0/1)# mls qos trust cos
DeviceA(config-if-GigabitEthernet 0/1)# no voice vlan mode auto
DeviceA(config-if-GigabitEthernet 0/1)# voice vlan enable
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

(7) Configure the uplink port GigabitEthernet 0/2 as a trunk port.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/2)# end
DeviceA# write
```

5. Verification

Run the **show voice vlan** command to check the current status of the voice VLAN on the device. GigabitEthernet 0/1 is manually added.

```
DeviceA# show voice vlan
Voice Vlan status: ENABLE
Voice Vlan ID       : 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1440 minutes
Voice Vlan cos      : 5
Voice Vlan dscp     : 40
Current voice vlan enabled port mode:
PORT               MODE
-------------------- ----------
Gi0/1              MANUAL
```

Check the voice VLAN OUI of the device.

```
DeviceA# show voice vlan oui
Oui           Mask            Description
0012.3400.0000  ffff.ff00.0000   B
```

Check port configuration.

```
DeviceA(config)#show interface swithport
Interface           Switchport Mode     Access Native Protected VLAN lists
-------------------- ---------- --------- ------ ------ ---------
----------------------
```

```
GigabitEthernet 0/1   enabled    Access    2      1      Disabled  ALL
GigabitEthernet 0/2   enabled    TRUNK     1      1      Disabled  ALL
```

6. Configuration Files

Device A configuration file

```
voice vlan 2
voice vlan cos 5
voice vlan dscp 40
voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description "B"
!
vlan range 1-2
!
interface GigabitEthernet 0/1
 switchport access vlan 2
 no voice vlan mode auto
 voice vlan enable
 mls qos trust cos
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

7. Common Errors

The trust mode of the QoS module is not enabled. Consequently, the packet priority modification cannot take effect, affecting voice traffic transmission.

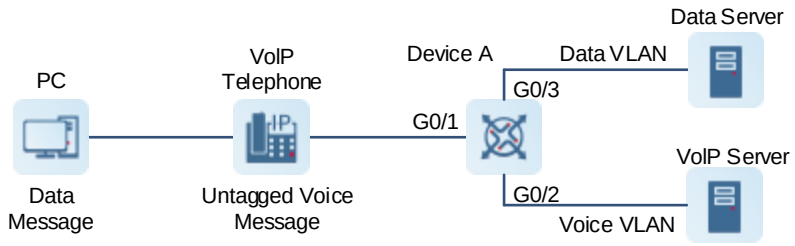
1.13.3 Configuring Isolation of Untagged Voice Traffic from Data Traffic

1. Requirements

A PC is connected to a VoIP telephone and the VoIP telephone is connected to device A. The VoIP telephone automatically obtains an IP address and sends untagged voice traffic. The PC sends untagged data traffic. To ensure quality of voice calls, the voice data must be transmitted in the dedicated voice VLAN 2 and this voice VLAN cannot transmit non-voice data. Common data is transmitted in VLAN 3 separately.

2. Topology

Figure 1-6 Network Topology of Isolation of Voice VLAN from Data VLAN



3. Notes

- Configure GigabitEthernet 0/1 to forward voice traffic and data traffic separately. Packets from the VoIP

telephone and PC are untagged. Therefore, configure the port as a hybrid port and enable data traffic to be forwarded in the native VLAN and voice traffic to be forwarded over the voice VLAN.

- The VoIP telephone connected to GigabitEthernet 0/1 sends untagged voice traffic. Therefore, set the voice VLAN to work in manual mode. The PC sends untagged data traffic. To isolate the data traffic from the voice traffic, enable the MAC VLAN function on GigabitEthernet 0/1 so that the port identifies the MAC address of the voice traffic and assigns the voice traffic to the voice VLAN.
- To ensure that the hybrid port receives untagged data traffic and voice traffic, add the data VLAN and voice VLAN to the allowed untagged VLAN list of the port.

4. Procedure

(1) A voice VLAN has been configured.

```
DeviceA>en
DeviceA# configure terminal
DeviceA(config)# vlan 2
DeviceA(config-vlan)# exit
DeviceA(config)# voice vlan 2
```

(2) Configure the device to identify packets with the OUI of 0012.3400.0000 and mask of ffff.ff00.0000 as voice packets and forward the packets to the voice VLAN.

```
DeviceA(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description B
```

(3) Configure MAC VLAN entries in global configuration mode so that voice traffic is forwarded to voice VLAN 2.

```
DeviceA(config)# mac-vlan mac-address 0012.3456.7890 mask ffff.ffff.ffff vlan 2
```

(4) Create data VLAN 3 to transmit common data.

```
DeviceA(config)# vlan 3
DeviceA(config-vlan)# exit
```

(5) Configure GigabitEthernet 0/1 as a hybrid port and data VLAN 3 as a native VLAN. In this way, the device sends untagged packets of data VLAN 3 and untagged packets of voice VLAN 2 to the user port.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode hybrid
DeviceA(config-if-GigabitEthernet 0/1)# switchport hybrid native vlan 3
DeviceA(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan add
untagged 2-3
```

(6) Enable the trust mode of the QoS module to trust packet priority modification. Set the voice VLAN of GigabitEthernet 0/1 to work in manual mode and enable the voice VLAN and MAC VLAN functions on the port.

```
DeviceA(config-if-GigabitEthernet 0/1)# mls qos trust cos
DeviceA(config-if-GigabitEthernet 0/1)# no voice vlan mode auto
DeviceA(config-if-GigabitEthernet 0/1)# voice vlan enable
DeviceA(config-if-GigabitEthernet 0/1)# mac-vlan enable
```

(7) Add GigabitEthernet 0/2 connected to the voice server to voice VLAN 2.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# switchport access vlan 2
```

```
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

(8) Configure GigabitEthernet 0/3 connected to the data server as a trunk port, and remove voice VLAN 2 from the allowed VLAN list of the port.

```
DeviceA(config)# interface gigabitethernet 0/3
DeviceA(config-if-GigabitEthernet 0/3)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/3)# switchport trunk allowed vlan remove 2
DeviceA(config-if-GigabitEthernet 0/3)# end
DeviceA# write
```

5. Verification

Check the current status of the voice VLAN on the device.

```
DeviceA# show voice vlan
Voice Vlan status: ENABLE
Voice Vlan ID: 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1440minutes
Voice Vlan cos: 6
Voice Vlan dscp: 46
Current voice vlan enabled port mode:
PORT                MODE
-------------------- ----------
Gi0/1               MANUAL
```

Check the OUI of the voice device.

```
DeviceA# show voice vlan oui
OUI           Mask          Description
--------------- --------------- ------------------------------
0012.3400.0000  ffff.ff00.0000  B
```

Check the MAC VLAN entries.

```
DeviceA# show mac-vlan all
The following MAC VLAN address exist:
S: Static   D: Dynamic
MAC ADDR       MASK          VLAN ID  PRIO  STATE
-----------------------------------------------------
0012.3456.7890  ffff.ffff.ffff  2       0    S
Total MAC VLAN address count: 1
```

6. Configuration Files

Device A configuration file

```
voice vlan 2
voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description "B"
mac-vlan mac-address 0012.3456.7890 mask ffff.ffff.ffff vlan 2
!
vlan range 1-3
!
```

```
interface GigabitEthernet 0/1
 switchport mode hybrid
 switchport hybrid native vlan 3
 switchport hybrid allowed vlan only tagged 1,4-4094
 switchport hybrid allowed vlan add untagged 2,3
 no voice vlan mode auto
 voice vlan enable
 mac-vlan enable
 mls qos trust cos
!
interface GigabitEthernet 0/2
 switchport access vlan 2
!
interface GigabitEthernet 0/3
 switchport mode trunk
 switchport trunk allowed vlan only 1,3-4094
!
```

Contents

1 Configuring GVRP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Background and Function 1
1.1.3 Principles 1
1.1.4 Basic Concepts 3
1.1.5 Packet Format 5
1.1.6 Protocols and Standards 6
1.2 Configuration Task Summary 6
1.3 Configuring Basic Features 6
1.3.1 Overview 6
1.3.2 Restrictions and Guidelines 6
1.3.3 Procedure 8
1.4 Configuring GVRP BPDU Tunnels 9
1.4.1 Overview 9
1.4.2 Restrictions and Guidelines 9
1.4.3 Procedure 9
1.5 Configuring Transparent Transmission of GVRP BPDU 10
1.5.1 Overview 10
1.5.2 Restrictions and Guidelines 10
1.5.3 Procedure 10
1.6 Monitoring 10

1.7 Configuration Examples.....11

1.7.1 Configuring Basic Functions of GVRP.....11

1.7.2 Configuring GVRP BPDU Tunnels.....16

1 Configuring GVRP

1.1 Introduction

1.1.1 Overview

Generic Attribute Registration Protocol (GARP) VLAN registration protocol (GVRP) is a protocol for dynamically configuring virtual local area network (VLAN) attributes. It propagates VLAN attributes through protocol packets, and implements automatic registration and deregistration of VLANs on an IEEE 802.1Q trunk port.

1.1.2 Background and Function

A network is huge and complex. It is impossible to learn the network topology and VLAN conditions in a short period of time, and manual configuration brings heavy workload and easily leads to errors. The GARP provides a mechanism to help the members of the same switching network to mutually distribute, propagate, and register information including VLAN and multicast address.

An application entity that complies with GARP is called a GARP application. At present, major GARP applications include GVRP and GARP Multicast Registration Protocol (GMRP). An application entity diffuses the attribute information through protocol data packets. The destination MAC address of protocol packets is the specific multicast MAC address. If a device supporting GARP receives packets of GARP application entities, it will distinguish different applications according to their destination MAC address, and then deliver the packets to different applications (GVRP or GMRP) for processing.

- GVRP is a GARP application. It can dynamically configure and diffuse VLAN attributes, and implements dynamic and automatic registration/deregistration of VLANs on an IEEE 802.1Q trunk port.
- GMRP is another GARP application. It provides a restricted multicast diffusion function similar to the IGMP probing technology.

With the VLAN automatic registration function of GVRP, you can configure the VLAN, and dynamically maintain the process of creating a VLAN and adding/deleting ports to/from a VLAN, ensuring the VLAN connectivity in the topology.

GVRP simplifies the VLAN configuration and management. It reduces the workload of manually configuring VLANs and adding ports to VLANs, and reduces the possibility of network disconnection due to inconsistent configuration.

1.1.3 Principles

1. Working Process

(1) GVRP advertising

If the GVRP function is enabled for a device and the advertising mode of the trunk port is **Normal**, the trunk port will regularly collect the VLAN information on the local port, encapsulate the information in GVRP packets and send them to the peer device, informing the peer device of the VLAN that the trunk port has joined or exited. The VLAN information type is GVRP Message Types, including Join message, Leave message, and LeaveAll message.

(2) GVRP registration (registration/deregistration)

The destination MAC address of a message packet is the specific multicast MAC address. After GVRP is enabled, the trunk port can recognize GVRP packets from other devices and obtain the VLAN registration or deregistration information by parsing the packets. If the registration mode is **Normal**, the port will create and join a VLAN dynamically, or the port will exit the VLAN and update the local VLAN registration information dynamically.

(3) GVRP advertisement diffusion

The device can also propagate the local VLAN registration information to other devices. The VLAN registration information includes the manually configured static registration information on the local device and the dynamic registration information from other devices. In this way, all devices in a VLAN maintain consistent VLAN information.

2. GVRP Advertising Modes

On a device with the GVRP function enabled, the trunk port decides to regularly collect or not collect VLAN information of the local port according to the advertising mode of the port (**Normal** or **Non-Applicant**). If the VLAN information is collected, the VLAN information is encapsulated in GVRP packets and sent to the peer device, informing the peer device of the VLAN where the device is. On such a basis, the peer device identifies the VLAN to be created.

- **Normal** mode: A device externally advertises its VLAN information, including dynamic and static VLAN information.
- **Non-Applicant** mode: A device does not advertise its VLAN information.

3. GVRP Registration Mode

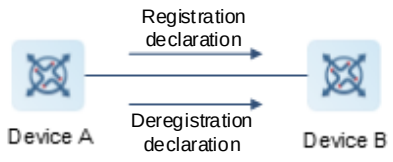
After receiving GVRP packets from the interconnected trunk port, the peer device parses the VLAN information and decides to process or not to process the VLAN information according to the port registration mode (**Normal** or **Disabled**).

- **Normal** mode: The device processes the VLAN information, dynamically creates a new VLAN and adds the port that receives the packet to the VLAN, or removes it from the VLAN.
- **Disabled** mode: The device does not process the VLAN information in the received GVRP packet.

4. VLAN Registration and Deregistration

Figure 1-1 shows the VLAN registration and deregistration process.

Figure 1-1 VLAN Registration and Deregistration



Device A sends a registration declaration to Device B through a GVRP advertisement, and the port of Device B receives the VLAN registration declaration and joins the VLAN contained in the declaration. This process is called VLAN registration.

Device A sends a deregistration declaration to Device B through a GVRP advertisement, and the port of Device B receives the VLAN deregistration declaration and exits the VLAN contained in the declaration. This process is called VLAN deregistration.

1.1.4 Basic Concepts

1. Static and Dynamic VLANs

- A manually created or deleted VLAN is a static VLAN.
- A VLAN dynamically created or deleted through GVRP is a dynamic VLAN.

The protocol state machine controls the process that a port joins or exits a dynamic VLAN. Only the trunk port that has received a GVRP registration or deregistration declaration can join or exit the dynamic VLAN created by GVRP; other trunk ports that have not received any GVRP registration or deregistration declaration cannot join or exit a dynamic VLAN, and even manual configuration cannot add or remove such a port to/from a dynamic VLAN.

The VLAN registration information propagated by GVRP includes the manually configured static registration information on the local device and the dynamic registration information from other devices. You can switch a dynamic VLAN to a static VLAN through configuration, but not the other way around.

2. Message Types

Terminals or bridge devices are GVRP members, and each port enabled with GVRP is called a GVRP application entity. The entities exchange information by transferring three types of messages.

- Join message

  The device sends a Join message in the following cases.

  - When a GVRP application entity wants other GVRP entities to register its own attribute information, it sends a Join message.
  - When a GVRP application entity receives a Join message from another GVRP entity, it sends a Join message for diffusion.
  - When a GVRP application entity is statically configured with attributes and requires other entities to register the attributes, it sends a Join message.

  Two types of Join messages are available: JoinEmpty and JoinIn. The differences between the two are as follows:

  - JoinEmpty message: Used to declare an unregistered attribute.
  - JoinIn message: Used to declare a registered attribute.

- Leave message

  The device sends a Leave message in the following cases.

  - When a GVRP application entity wants other GVRP entities to deregister its own attribute information, it sends a Leave message.
  - When a GVRP application entity receives a Leave message from another GVRP entity, it sends a Leave message.
  - When a GVRP application entity statically deregisters VLAN attributes and requires other entities to deregister the attributes, it sends a Leave message.

Two types of Leave messages are available: LeaveEmpty and LeaveIn. The differences between the two are as follows:

- LeaveEmpty message: Used to deregister an unregistered attribute.
- LeaveIn message: Used to deregister a registered attribute.

- LeaveAll message

  After GVRP is enabled, each GVRP application entity will enable its own LeaveAll timer. If the LeaveAll timer of a GVRP entity times out, it will send a LeaveAll message to deregister all attributes, which will cause other GVRP entities to re-register the attribute information. If a GVRP entity receives a LeaveAll message from another entity, it will send a LeaveAll message and restart the LeaveAll timer to initiate a new cycle.

3. Timer Types

GVRP defines four timers to control GVRP message sending.

- Hold timer

  The Hold timer defines the maximum delay interval *hold* before a port sends a Join message or Leave message. When a GVRP application entity has its attributes changed or receives a GVRP message from another entity, it enables the Hold timer. During the timeout period, the GVRP encapsulates all GVRP messages to be sent into packets as few as possible, and sends the packets when the timer times out. This reduces the quantity of sent packets and saves bandwidth resources. The interval is from 0 to *hold*.

- Join timer

  The Join timer defines the waiting time for Join message retransmission, conductive to ensuring the reliability of Join message transmission. After sending a Join message, the GVRP application entity will wait for a Join timer interval. If it receives a JoinIn message sent from another entity before the Join timer times out, it will not resend the Join message; otherwise, it will resend the Join message. Each GVRP application entity has one Join timer, and all attributes share one Join timer.

- Leave timer

  The Leave timer defines the waiting time from receiving a Leave message by the port to deleting the port from the VLAN, which helps to avoid frequent network changes. If the GVRP application entity wants other entities to deregister its VLAN attribute information, it will send a Leave message; the entity receiving the message will enable the Leave timer, and, if the port does not receive the Join message of the attribute information after the Leave timer times out, the state of the port becomes **Empty** and the port is removed from the VLAN member list; if the port receives the Join message of the attribute information before the Leave timer times out, the port will not be removed from the VLAN and the timer will time out.

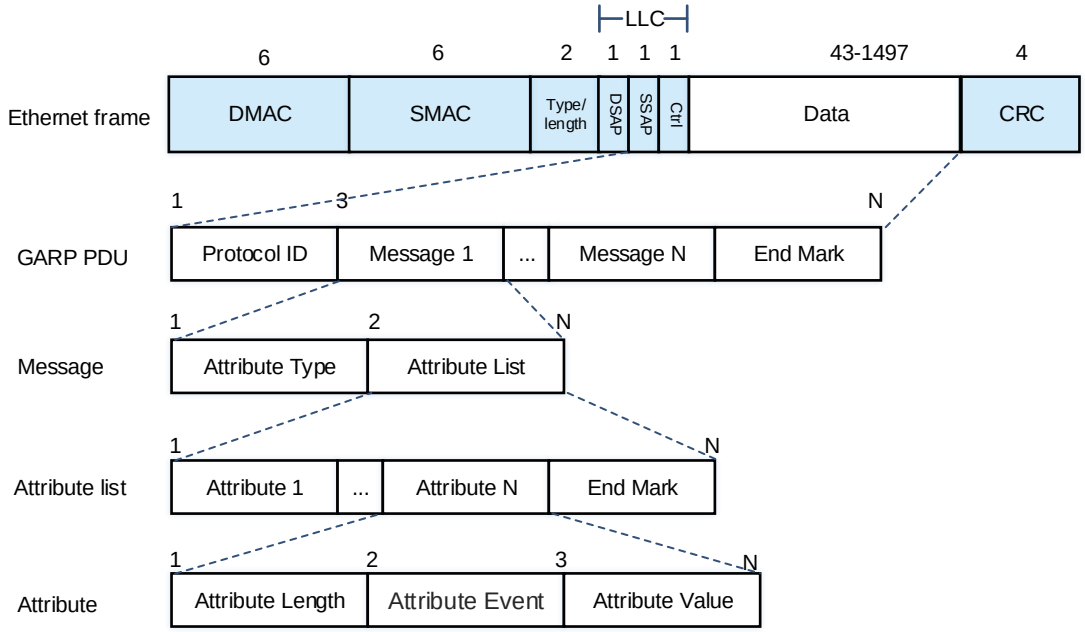
- LeaveAll timer

  The LeaveAll timer defines the minimum time interval *leaveall* for the port to send a LeaveAll message. Each GVRP application entity enables its own LeaveAll timer when the entity is enabled. If the LeaveAll timer times out, the GVRP application entity will send a LeaveAll message to instruct other entities to re-register the attribute information. The interval ranges from *leaveall* to the sum of *leaveall* and *hold*. The LeaveAll message is also sent to the local port to trigger the Leave timer to start timing again and initiate a new cycle; if the port receives the LeaveAll message before the timer times out, the timer restarts timing.

1.1.5 Packet Format

The GVRP protocol packets are encapsulated in Ethernet frames. Figure 1-2 shows the packet format.

Figure 1-2 GVRP Packet Format of Ethernet Frame



The following table describes the meaning of each GVRP Ethernet frame field.

Table 1-1 Meanings of GVRP Ethernet Frame Fields

Field	Number of Bytes	Description
Protocol ID	2	Indicates the protocol ID, 0x0001.
Message	N	Indicates a message. Each message consists of the attribute type and attribute list.
Attribute Type	1	Indicates the attribute type, defined by the specific GARP application. 0x01: Indicates GVRP application, and **Attribute Value** is **VLAN ID**.
Attribute List	N	Indicates the attribute list, composed of multiple attributes and the end mark.
Attribute	N	Indicates an attribute. Each attribute consists of the attribute length, attribute event, and attribute value.
Attribute Length	1	Indicates the attribute length. The value range is from 0x02 to 0xFF, that is, from 2 to 255.

Field	Number of Bytes	Description
Attribute Event	1	Indicates the event described by the attribute: 0x00: LeaveAll Event 0x01: JoinEmpty Event 0x02: JoinIn Event 0x03: LeaveEmpty Event 0x04: LeaveIn Event 0x05: Empty Event
Attribute Value	N	Indicates the attribute value. The attribute value of GVRP is **VLAN ID**, but the attribute value of **LeaveAll** is invalid.
End Mark	1	Indicates the end mark of GVRP PDU, expressed using 0x00.

1.1.6 Protocols and Standards

- IEEE 802.1D: IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges
- IEEE 802.1Q: IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks

1.2 Configuration Task Summary

- When the GVRP function is enabled, configuration includes the following tasks:
  - a Configuring Basic Features
  - b (Optional) Configuring GVRP BPDU Tunnels
- When the GVRP function is disabled, configuration includes the following tasks:
  - (Optional) Configuring Transparent Transmission of GVRP BPDU

1.3 Configuring Basic Features

1.3.1 Overview

The GVRP function is used to dynamically create or delete VLANs and add or remove ports to/from VLANs. Devices synchronize respective VLAN information to maintain communication in the topology. This function can reduce the manual configuration workload and simplify VLAN management.

1.3.2 Restrictions and Guidelines

- GVRP needs to be enabled on the two devices connected for communication. The GVRP function takes effect only on trunk ports. All the VLANs created by GVRP are tagged VLANs. GVRP information is transmitted only by trunk Links. The transmitted information contains the information on all VLANs on the current device, including dynamically learned VLANs and manually configured VLANs. The VLAN

information that is dynamically learned by GVRP is saved in the memory temporarily, but not in the flash memory of the system. When the device is reset, all the information will be lost. Users cannot save the VLAN information that is dynamically learned.

- The relationship between GVRP and Spanning Tree Protocol (STP) is as follows.
  - If STP is not enabled, all available ports can participate in GVRP.
  - If STP is enabled, only ports in **Forwarding** state participate in GVRP (receiving and sending GVRP BPDU packets) and have their VLAN information diffused by GVRP.
  - If Multi Spanning Tree Protocol (MSTP) is enabled, GVRP can run in the spanning tree context to which VLAN1 belongs. You cannot specify other spanning tree context for GVRP.
  - If Single Spanning Tree Protocol (SSTP) is enabled, only ports in **Forwarding** state in the current spanning tree context participate in GVRP.
- Enable the function of creating VLAN dynamically.
  - The parameters of a dynamic VLAN created through GVRP cannot be modified manually.
  - When a port receives a JoinIn or JoinEmpty message containing a locally non-existent VLAN, GVRP may create this VLAN. After this function is enabled, when the device receives the Join message from GVRP, a VLAN will be created dynamically.
- Configure the registration mode of a port.
  - To enable dynamic VLAN registration on a port, run the **gvrp registration mode normal** command. To disable dynamic VLAN registration on a port, run the **gvrp register mode disable** command.
  - If dynamic VLAN registration is enabled, dynamic VLANs will be created on the local device when the port receives a GVRP packet carrying VLAN information from the peer end. If dynamic VLAN registration is disabled, no dynamic VLAN will be created on the local device when the port receives a GVRP packet from the peer end.
  - The two registration modes do not affect the static VLANs on the port. The registration mode for manually created static VLANs is always **Fixed Registrar**.
- Configure the timers.
  - GVRP uses the Hold, Leave, and LeaveAll timers to define the sending interval of various types of packets. The timers are controlled by the GVRP state machine and can be triggered by each other. The three timers are subject to this relationship: 3 x Hold ≤ Leave ≤ LeaveAll.
  - All devices that need to exchange GVRP information on the network must have consistent GVRP timer configuration; otherwise, the GVRP function will not take effect.
- Enable the GVRP function.
  - After the GVRP function is enabled, the device sends GVRP packets carrying VLAN information. After GVRP is disabled, the device does not send GVRP packets carrying VLAN information or process received GVRP packets.
  - When GVRP is not enabled globally, GVRP configuration not take effect. Only when GVRP is enabled globally, will GVRP configuration take effect.
  - The information of super VLAN and sub VLAN cannot be synchronized to the interconnected devices through GVRP.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of creating VLANs dynamically.

gvrp dynamic-vlan-creation enable

Creating VLANs dynamically is disabled by default.

(4) (Optional) Configure the GVRP timer.

gvrp timer { **join** *hold* | **leave** *leave* | **leaveall** *leaveall* }

By default, the maximum delay before a port sends a Join or Leave message is 200 ms, the waiting time from receiving a Leave message by the port to deleting the port from the VLAN is 600 ms, and the minimum time interval for the port to send a LeaveAll message is 10,000 ms.

(5) Configure the interconnection interface as trunk port (the GVRP function takes effect only on trunk ports after being enabled globally).

a Enter the interface configuration mode.

interface *interface-type interface-number*

b Configure the port mode as trunk port.

switchport mode trunk

An interface works in access mode by default.

c Return to the global configuration mode.

exit

(6) Enable the GVRP function globally.

gvrp enable

The GVRP function is disabled by default.

(7) (Optional) Configure the advertising mode of a port.

a Enter the interface configuration mode.

interface *interface-type interface-number*

b Configure the advertising mode of a port.

gvrp applicant state { **normal** | **non-applicant** }

The advertising mode of a port is **Normal** by default, namely, advertisement will be sent.

c Return to the global configuration mode.

exit

(8) (Optional) Configure the registration mode of a port.

a Enter the interface configuration mode.

interface *interface-type interface-number*

b Configure the registration mode of a port.

gvrp registration mode { **normal** | **disable** }

The registration mode of a port is **Normal** by default, namely, VLAN information will be updated dynamically.

c Return to the global configuration mode.

exit

1.4 Configuring GVRP BPDU Tunnels

1.4.1 Overview

In the QinQ network, if GVRP of the user network and the SP network needs to be calculated separately without interfering with each other, you can configure the GVRP BPDU tunnel so that the GVRP packets of the user network can be transmitted through the SP network tunnel.

The destination MAC address of GVRP BPDU packets is the dedicated multicast address 0180.c200.0006. To avoid impact on the SP network by GVRP packets of the user network, when GVRP packets of the user network enter an edge device of the SP network, the edge device changes the destination MAC address of the packets from the GVRP dedicated address (0180.c200.0006) to the tunnel address (01d0.f800.0006 by default) before forwarding on the SP network. After the packets are forwarded to an edge device at the other end, the destination MAC address is restored from the tunnel address (01d0.f800.0006 by default) to the GVRP dedicated address (0180.c200.0006), and the packets are forwarded to the user network at the other end. In this way, the GVRP packets of the user network are transmitted through the tunnel of the SP network.

1.4.2 Restrictions and Guidelines

- The tunnel function takes effect only when the GVRP BPDU tunnel is enabled in both global configuration mode and interface configuration mode. In the global configuration mode, run the **l2protocol-tunnel gvrp** command to enable the GVRP BPDU tunnel function globally. In interface configuration mode, run the **l2protocol-tunnel gvrp enable** command to enable the GVRP BPDU tunnel function on a port.
- The optional tunnel addresses of GVRP packets are 01d0.f800.0006 (default value) and 011a.a900.0006.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the configuration mode of the interface connected to the user network.

interface *interface-type interface-number*

(4) Enable the GVRP BPDU tunnel function on a port.

l2protocol-tunnel gvrp enable

The GVRP BPDU tunnel function of a port is disabled by default.

(5) Return to the global configuration mode.

exit

(6) (Optional) Configure an address for the GVRP tunnel.

l2protocol-tunnel gvrp tunnel-dmac *mac-address*

The GVRP tunnel address is 01d0.f800.0006 by default.

(7) Enable the GVRP BPDU tunnel function globally.

l2protocol-tunnel gvrp

The global GVRP BPDU tunnel function is disabled by default.

1.5 Configuring Transparent Transmission of GVRP BPDU

1.5.1 Overview

In IEEE 802.1Q, the destination MAC address of GVRP BPDU packets is the dedicated multicast address 0180.c200.0006. Generally, devices complying with IEEE 802.1Q do not forward GVRP BPDU frames with the destination MAC address 0180.c200.0006, no matter whether GVRP is enabled. If the device has GVRP enabled, it will use GVRP BPDU frames for GVRP calculation; otherwise, it will discard GVRP packets.

However, in specific applications, devices may be required to transparently transmit GVRP packets. For example, a device does not have GVRP enabled, but the device interconnected to it has GVRP enabled. To enable the devices at both ends to perform GVRP calculation normally, the local device needs to transparently transmit GVRP BPDU frames. In this case, the GVRP BPDU transparent transmission function can be enabled to allow the device to forward the packets with the destination MAC address of 0180.c200.0006.

1.5.2 Restrictions and Guidelines

The GVRP BPDU transparent transmission function takes effect only when GVRP is disabled. When the device has GVRP enabled, this function cannot be used to transparently transmit GVRP BPDU frames. For example, in the QinQ network, both the SP network device and the user network device have GVRP enabled. If the SP network device needs to forward GVRP packets of the user network but does not forward GVRP packets of the SP network, the GVRP BPDU tunnel function is needed.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the transparent transmission function of GVRP BPDU packets.

bridge-frame forwarding protocol gvrp

The transparent transmission function of GVRP BPDU packets is disabled by default.

1.6 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

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

You can run the **clear** commands to clear information.

Caution

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

Table 1-2 Monitoring

Command	Purpose
clear gvrp statistics { *interface-type interface-number* | **all** }	Clears port statistics.
show gvrp statistics { *interface-type interface-number* | **all** }	Displays port statistics.
show gvrp status	Displays the current GVRP status.
show gvrp configuration	Displays the current GVRP configuration.
show l2protocol-tunnel gvrp	Displays the GVRP BPDU tunnel information.
debug gvrp event	Enables the GVRP event debugging function.
debug gvrp timer	Enables the GVRP timer debugging function.

1.7 Configuration Examples

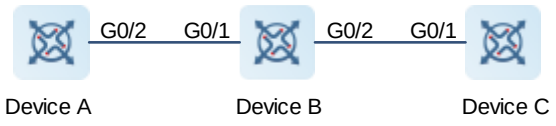
1.7.1 Configuring Basic Functions of GVRP

1. Requirements

The GVRP function is enabled in a topology to dynamically maintain the VLANs and the VLAN-port relationship.

2. Topology

Figure 1-3 Application Scenario of GVRP Basic Function



3. Notes

- On Devices A and C, configure VLANs used for communication on the user network.
- Enable GVRP on Devices A, B, and C, and enable the dynamic creation function of VLAN.
- Configure the ports connected between Devices A, B, and C as trunk ports, and ensure that the permitted VLAN lists of trunk ports include the communication VLANs.
- You are advised to enable STP to avoid loops.

4. Procedure

(1) Create VLANs for user network communication.

Create VLANs 2 to 10 for user network communication on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan range 2-10
DeviceA(config-vlan)# exit
```

Create VLANs 11 to 20 for user network communication on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# vlan range 11-20
DeviceC(config-vlan)# exit
```

(2) Enable the dynamic creation function of VLAN.

Enable the dynamic creation function of VLAN on Device A.

```
DeviceA(config)# gvrp dynamic-vlan-creation enable
```

Enable the dynamic creation function of VLAN on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# gvrp dynamic-vlan-creation enable
```

Enable the dynamic creation function of VLAN on Device C.

```
DeviceC(config)# gvrp dynamic-vlan-creation enable
```

(3) Configure the ports for connecting to the devices as trunk ports.

Configure the ports for the interconnected devices as trunk ports on Device A.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# switchport
DeviceA(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

Configure the ports for the interconnected devices as trunk ports on Device B.

```
DeviceB(config)# interface range gigabitethernet 0/1-2
DeviceB(config-if-range)# switchport
DeviceB(config-if-range)# switchport mode trunk
DeviceB(config-if-range)# exit
```

Configure the ports for the interconnected devices as trunk ports on Device C.

```
DeviceC(config)# interface gigabitethernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# switchport
DeviceC(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceC(config-if-GigabitEthernet 0/1)# exit
```

(4) Enable the GVRP function.

Enable the GVRP function on Device A.

```
DeviceA(config)# gvrp enable
```

Enable the GVRP function on Device B.

```
DeviceB(config)# gvrp enable
```

Enable the GVRP function on Device C.

```
DeviceC(config)# gvrp enable
```

5. Verification

(1) Before the GVRP function is enabled globally, check the static VLAN configuration of the device; check whether the interconnection ports are trunk ports and allow all VLANs to pass.

Only static VLANs exist on Device A; the interconnection port GigabitEthernet 0/2 is a trunk port and allows all VLANs to pass.

```
DeviceA# show vlan
VLAN        Name                  Status        Ports
----------  ---------------------  ------------  --------------------------
       1   VLAN0001              STATIC       Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                            Gi0/5, Gi0/6, Gi0/7, Gi0/8
     2-10   VLAN0002-VLAN0010       STATIC       Gi0/2
DeviceA# show interface gigabitethernet 0/2 switchport
Interface               Switchport Mode     Access Native Protected VLAN lists
------------------------- ---------- --------- ------ ------ ---------
--------------------
GigabitEthernet 0/2       enabled    TRUNK     1      1      Disabled  ALL
```

Only a static VLAN exists on Device B; the interconnection ports GigabitEthernet 0/1 and GigabitEthernet 0/2 are trunk ports and allow all VLANs to pass.

```
DeviceB# show vlan
VLAN        Name                  Status        Ports
----------  ---------------------  ------------  --------------------------
       1   VLAN0001              STATIC       Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                            Gi0/5, Gi0/6, Gi0/7, Gi0/8
DeviceB# show interface switchport
Interface               Switchport Mode     Access Native Protected VLAN lists
------------------------- ---------- --------- ------ ------ ---------
--------------------
GigabitEthernet 0/1       enabled    TRUNK     1      1      Disabled  ALL
GigabitEthernet 0/2       enabled    TRUNK     1      1      Disabled  ALL
```

Only static VLANs exist on Device C; the interconnection port GigabitEthernet 0/1 is a trunk port and allows all VLANs to pass.

```
DeviceC# show vlan
VLAN        Name                  Status        Ports
----------  ---------------------  ------------  --------------------------
       1   VLAN0001              STATIC       Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                            Gi0/5, Gi0/6, Gi0/7, Gi0/8
    11-20   VLAN0011-VLAN0020       STATIC       Gi0/1
DeviceA# show interface gigabitethernet 0/1 switchport
Interface               Switchport Mode     Access Native Protected VLAN lists
-------------------------- ---------- --------- ------ ------ ---------
--------------------
GigabitEthernet 0/1       enabled   TRUNK    1     1     Disabled  ALL
```

(2) After the GVRP function is enabled globally, check the GVRP configuration of devices.

Check whether the GVRP function of Device A has been enabled, and the trunk port normally advertises the GVRP information and dynamically updates the VLAN information.

```
DeviceA# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP dynamic VLAN creation:enabled
Join Timers(ms):200
Leave Timers(ms):600
Leaveall Timers(ms):1000
Port based GVRP Configuration:
       PORT            Applicant Status        Registration Mode
-----------------------  --------------------    ---------------------
GigabitEthernet 0/2          normal                 normal
```

Check whether the GVRP function of Device B has been enabled, and the trunk port normally advertises the GVRP information and dynamically updates the VLAN information.

```
DeviceB# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP dynamic VLAN creation:enabled
Join Timers(ms):200
Leave Timers(ms):600
Leaveall Timers(ms):1000
Port based GVRP Configuration:
       PORT            Applicant Status        Registration Mode
-----------------------  --------------------    ---------------------
GigabitEthernet 0/1         normal                 normal
GigabitEthernet 0/2         normal                 normal
```

Check whether the GVRP function of Device C has been enabled, and the trunk port normally advertises the GVRP information and dynamically updates the VLAN information.

```
DeviceC# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
```

```
GVRP dynamic VLAN creation:enabled
Join Timers(ms):200
Leave Timers(ms):600
Leaveall Timers(ms):1000
Port based GVRP Configuration:
       PORT            Applicant Status        Registration Mode
----------------------- --------------------    ---------------------
GigabitEthernet 0/1          normal                 normal
```

(3) After the GVRP function is enabled globally, check the VLANs dynamically created by devices and check whether the trunk ports join dynamic VLANs.

Dynamic VLANs 11 to 20 are created on Device A, and the trunk port Gigabit Ethernet 0/2 joins the dynamic VLANs 11 to 20.

```
DeviceA(config)# show vlan
VLAN        Name                  Status        Ports
----------  ---------------------  ------------  --------------------------
       1   VLAN0001              STATIC       Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                            Gi0/5, Gi0/6, Gi0/7, Gi0/8
     2-10   VLAN0002-VLAN0010       STATIC       Gi0/2
    11-20   DVLAN0011-DVLAN0020     DYNAMIC      Gi0/2
```

Dynamic VLANs 2 to 20 are created on Device B, and the trunk ports GigabitEthernet 0/1 and GigabitEthernet 0/2 join the dynamic VLANs 2 to 20.

```
DeviceB(config)# show vlan
VLAN        Name                  Status        Ports
----------  ---------------------  ------------  --------------------------
       1   VLAN0001              STATIC       Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                            Gi0/5, Gi0/6, Gi0/7, Gi0/8
     2-20   DVLAN0002-DVLAN0020     DYNAMIC      Gi0/1, Gi0/2
```

Dynamic VLANs 2 to 10 are created on Device C, and the trunk port Gigabit Ethernet 0/1 joins the dynamic VLANs 2 to 10.

```
DeviceC(config)# show vlan
VLAN        Name                  Status        Ports
----------  ---------------------  ------------  --------------------------
       1   VLAN0001              STATIC       Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                            Gi0/5, Gi0/6, Gi0/7, Gi0/8
     2-10   DVLAN0002-DVLAN0010     DYNAMIC      Gi0/1
    11-20   VLAN0011-VLAN0020       STATIC       Gi0/1
```

6. Configuration Files

- Device A configuration file

```
gvrp enable
gvrp dynamic-vlan-creation enable
!
vlan range 1-10
!
```

```
interface GigabitEthernet 0/2
 switchport mode trunk
```

- Device B configuration file

```
gvrp enable
gvrp dynamic-vlan-creation enable
!
vlan range 1
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

- Device C configuration file

```
gvrp enable
gvrp dynamic-vlan-creation enable
!
vlan range 1,11-20
!
interface GigabitEthernet 0/1
 switchport mode trunk
```

7. Common Errors

- The interconnection ports of devices are not in trunk mode.
- The permitted VLAN list of the interconnection ports of devices does not contain the user communication VLANs.
- The GVRP advertising mode and registration mode of trunk ports are not set to **Normal**.

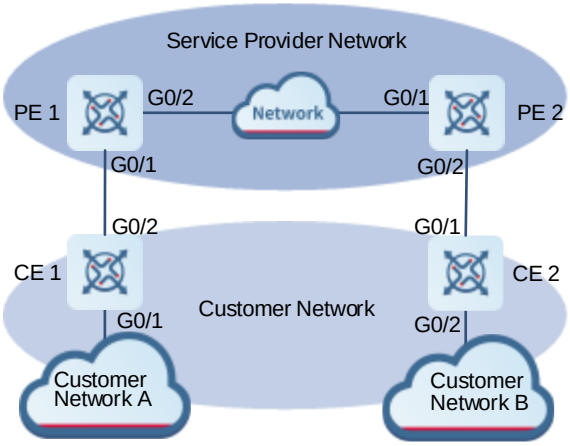
1.7.2 Configuring GVRP BPDU Tunnels

1. Requirements

The GVRP packets of the user network are transmitted through the tunnel of the SP network.

2. Topology

Figure 1-4 Application Scenario of GVRP BPDU Tunnel Function



3. Notes

- Configure the basic functions of GVRP on PE 1 and PE 2, including enabling the dynamic creation function of VLAN, configuring the interconnection port GigabitEthernet 0/5 as trunk port, and enabling the GVRP function globally.
- Enable the basic QinQ function on the ports connected to the user network on PE 1 and PE 2 so that data packets of the user network are transmitted within VLAN 200 on the SP network.
- Enable the GVRP tunnel function on the ports connected to the user network on PE 1 and PE 2 so that the SP network can transmit GVRP packets of the user network through the GVRP BPDU tunnel.

4. Procedure

(1) Configure the basic functions of GVRP on the interconnection ports of SP devices.

Enable the GVRP function on PE 1 and Gigabit Ethernet 0/2 in turn.

```
PE1> enable
PE1# configure terminal
PE1(config)# vlan 251
PE1(config-vlan)# exit
PE1(config)# gvrp dynamic-vlan-creation enable
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-GigabitEthernet 0/2)# switchport
PE1(config-if-GigabitEthernet 0/2)# switchport mode trunk
PE1(config-if-GigabitEthernet 0/2)# exit
PE1(config)# gvrp enable
```

Enable the GVRP function on PE 2 and Gigabit Ethernet 0/1 in turn.

```
PE2> enable
PE2# configure terminal
PE2(config)# vlan 252
PE2(config-vlan)# exit
```

```
PE2(config)# gvrp dynamic-vlan-creation enable
PE2(config)# interface gigabitethernet 0/1
PE2(config-if-GigabitEthernet 0/1)# switchport
PE2(config-if-GigabitEthernet 0/1)# switchport mode trunk
PE2(config-if-GigabitEthernet 0/1)# exit
PE2(config)# gvrp enable
```

(2) Configure the basic QinQ function on SP devices. Use VLAN 250 to encapsulate the packets of users at two ends.

Configure the basic QinQ encapsulation on the port Gigabit Ethernet 0/1 connected to the user on PE 1.

```
PE1(config)# vlan 250
PE1(config-vlan)# exit
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-GigabitEthernet 0/1)# switchport
PE1(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
PE1(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel native vlan 250
PE1(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan add
untagged 250
```

Configure the basic QinQ encapsulation on the port Gigabit Ethernet 0/2 connected to the user on PE 2.

```
PE2(config)# vlan 250
PE2(config-vlan)# exit
PE2(config)# interface gigabitethernet 0/2
PE2(config-if-GigabitEthernet 0/2)# switchport
PE2(config-if-GigabitEthernet 0/2)# switchport mode dot1q-tunnel
PE2(config-if-GigabitEthernet 0/2)# switchport dot1q-tunnel native vlan 250
PE2(config-if-GigabitEthernet 0/2)# switchport dot1q-tunnel allowed vlan add
untagged 250
```

(3) Enable the GVRP tunnel on SP devices.

Enable the GVRP tunnel on port Gigabit Ethernet 0/1 of PE 1 and globally in turn.

```
PE1(config-if-GigabitEthernet 0/1)# l2protocol-tunnel gvrp enable
PE1(config-if-GigabitEthernet 0/1)# exit
PE1(config)# l2protocol-tunnel gvrp
```

Enable the GVRP tunnel on port Gigabit Ethernet 0/2 of PE 2 and globally in turn.

```
PE2(config-if-GigabitEthernet 0/2)# l2protocol-tunnel gvrp enable
PE2(config-if-GigabitEthernet 0/2)# exit
PE2(config)# l2protocol-tunnel gvrp
```

(4) Configure the basic functions of GVRP on user network devices.

Enable the GVRP function on CE 1 and port Gigabit Ethernet 0/2 in turn.

```
CE1> enable
CE1# configure terminal
CE1(config)# vlan range 60-69
CE1(config-vlan)# exit
CE1(config)# gvrp dynamic-vlan-creation enable
CE1(config)# interface gigabitethernet 0/2
```

```
CE1(config-if-GigabitEthernet 0/2)# switchport
CE1(config-if-GigabitEthernet 0/2)# switchport mode trunk
CE1(config-if-GigabitEthernet 0/2)# exit
CE1(config)# gvrp enable
```

Enable the GVRP function on CE 2 and port Gigabit Ethernet 0/1 in turn.

```
CE2> enable
CE2# configure terminal
CE2(config)# vlan range 70-79
CE2(config-vlan)# exit
CE2(config)# gvrp dynamic-vlan-creation enable
CE2(config)# interface gigabitethernet 0/1
CE2(config-if-GigabitEthernet 0/1)# switchport
CE2(config-if-GigabitEthernet 0/1)# switchport mode trunk
CE2(config-if-GigabitEthernet 0/1)# exit
CE2(config)# gvrp enable
```

5. Verification

(1) Before the GVRP function is enabled globally, check the static VLAN configuration of the device; check whether the ports for advertising and processing GVRP packets are trunk ports and allow all VLANs to pass.

Only static VLANs exist on PE 1; the uplink port Gigabit Ethernet 0/2 is a trunk port and allows all VLANs to pass.

```
PE1# show vlan
VLAN      Name                          Status    Ports
---------- -------------------------------- ---------
-----------------------------------
       1 VLAN0001                      STATIC    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                              Gi0/5, Gi0/6, Gi0/7, Gi0/8
     250 VLAN0250                      STATIC    Gi0/1, Gi0/2
     251 VLAN0251                      STATIC    Gi0/2
PE1# show interface switchport
Interface              Switchport Mode     Access Native Protected VLAN lists
------------------------ ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1     enabled    TUNNEL    1      250    Disabled  1,250
GigabitEthernet 0/2     enabled    TRUNK     1      1      Disabled  ALL
```

Only static VLANs exist on PE 2; the uplink port Gigabit Ethernet 0/1 is a trunk port and allows all VLANs to pass.

```
PE2# show vlan
VLAN      Name                          Status    Ports
---------- -------------------------------- ---------
-----------------------------------
       1 VLAN0001                      STATIC    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                              Gi0/5, Gi0/6, Gi0/7, Gi0/8
     250 VLAN0250                      STATIC    Gi0/1, Gi0/2
     252 VLAN0252                      STATIC    Gi0/1
```

```
PE2# show interface switchport
Interface             Switchport Mode     Access Native Protected VLAN lists
----------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1    enabled    TRUNK    1     1     Disabled  ALL
GigabitEthernet 0/2    enabled    TUNNEL   1     250    Disabled  1,250
```

Only static VLANs exist on GE 1; the unlink port Gigabit Ethernet 0/2 is a trunk port and allows all VLANs to pass.

```
CE1# show vlan
VLAN      Name                        Status    Ports
---------- -------------------------------- ---------
------------------------------------
       1 VLAN0001                     STATIC    Gi0/1,Gi0/2, Gi0/3, Gi0/4
                                              Gi0/5, Gi0/6, Gi0/7, Gi0/8
    60-69 VLAN0060-VLAN0069             STATIC    Gi0/2
CE1# show interface switchport
Interface             Switchport Mode     Access Native Protected VLAN lists
----------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/2     enabled    TRUNK    1     1     Disabled  ALL
```

Only static VLANs exist on CE 2; the uplink port Gigabit Ethernet 0/1 is a trunk port and allows all VLANs to pass.

```
CE2# show vlan
VLAN      Name                        Status    Ports
---------- -------------------------------- ---------
------------------------------------
       1 VLAN0001                     STATIC    Gi0/1,Gi0/2, Gi0/3, Gi0/4
                                              Gi0/5, Gi0/6, Gi0/7, Gi0/8
    70-79 VLAN0070-VLAN0079             STATIC    Gi0/1
CE2# show interface switchport
Interface             Switchport Mode     Access Native Protected VLAN lists
----------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1    enabled    TRUNK    1     1     Disabled  ALL
```

(2) Check whether the QinQ function is enabled, the SP device port connected to the user is the Dot1q-tunnel port, and the GVRP tunnel function is enabled.

Check the GVRP BPDU tunnel configuration on PE 1, and check whether the interface type is **Dot1q-tunnel**.

```
PE1# show interfaces dot1q-tunnel
========Interface Gi0/1========
Native vlan: 250
Allowed vlan list:1,250,
Tagged vlan list:
```

```
PE1# show l2protocol-tunnel gvrp
L2protocol-tunnel: Gvrp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0006
GigabitEthernet 0/1 l2protocol-tunnel gvrp enable
```

Check the GVRP BPDU tunnel configuration on PE 2, and check whether the interface type is **Dot1q-tunnel**.

```
PE2# show interfaces dot1q-tunnel
========Interface Gi0/2========
Native vlan: 250
Allowed vlan list:1,250,
Tagged vlan list:

PE2# show l2protocol-tunnel gvrp
L2protocol-tunnel: Gvrp Enable
L2protocol-tunnel destination mac address:01d0.f800.0006
GigabitEthernet 0/2 l2protocol-tunnel gvrp enable
```

(3) After the GVRP function is enabled globally using the **gvrp enable** command, check the GVRP configuration of devices.

Check whether the GVRP function of PE 1 has been enabled, and the trunk port normally advertises the GVRP information and dynamically updates the VLAN information.

```
PE1# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP Dynamic VLAN Creation:enabled
Join Timers(ms):200
Leave Timers(ms):600
Leaveall Timers(ms):10000
Port based GVRP Configuration:
       PORT            Applicant Status        Registration Mode
----------------------  --------------------    ---------------------
GigabitEthernet 0/2          normal                 normal
```

Check whether the GVRP function of PE 2 has been enabled, and the trunk port normally advertises the GVRP information and dynamically updates the VLAN information.

```
PE2# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP Dynamic VLAN Creation:enabled
Join Timers(ms):200
Leave Timers(ms):600
Leaveall Timers(ms):10000
Port based GVRP Configuration:
       PORT            Applicant Status        Registration Mode
----------------------  --------------------    ---------------------
GigabitEthernet 0/1          normal                 normal
```

Check whether the GVRP function of CE 1 has been enabled, and the trunk port normally advertises the GVRP information and dynamically updates the VLAN information.

```
CE1# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP Dynamic VLAN Creation:enabled
Join Timers(ms):200
Leave Timers(ms):600
Leaveall Timers(ms):10000
Port based GVRP Configuration:
       PORT            Applicant Status        Registration Mode
-----------------------  --------------------    ---------------------
GigabitEthernet 0/2          normal                 normal
```

Check whether the GVRP function of CE 2 has been enabled, and the trunk port normally advertises the GVRP information and dynamically updates the VLAN information.

```
CE2# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP Dynamic VLAN Creation:enabled
Join Timers(ms):200
Leave Timers(ms):600
Leaveall Timers(ms):10000
Port based GVRP Configuration:
       PORT            Applicant Status        Registration Mode
-----------------------  --------------------    ---------------------
GigabitEthernet 0/1          normal                 normal
```

(4) After the GVRP function is enabled globally, check whether SP network devices can dynamically create VLANs on them; VLANs of user network will not be created dynamically. It indicates that the GVRP packets of user network do not affect the GVRP operation of SP devices.

Dynamic VLAN 252 has been created on PE 1, and the trunk port Gigabit Ethernet 0/2 joins the dynamic VLAN 252.

```
PE1(config)# show vlan
VLAN      Name                          Status    Ports
---------- ------------------------------- ---------
------------------------------------
        1 VLAN0001                      STATIC    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                                 Gi0/5, Gi0/6, Gi0/7, Gi0/8
      250 VLAN0250                      STATIC    Gi0/1, Gi0/2
      251 VLAN0251                      STATIC    Gi0/2
      252 DVLAN0252                     DYNAMIC   Gi0/2
```

Dynamic VLAN 251 has been created on PE 2, and the trunk port Gigabit Ethernet 0/1 joins the dynamic VLAN 251.

```
PE2(config)# show vlan
VLAN      Name                          Status    Ports
```

```
---------- -------------------------------- ---------
-----------------------------------
       1 VLAN0001                      STATIC    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                              Gi0/5, Gi0/6, Gi0/7, Gi0/8
     250 VLAN0250                      STATIC    Gi0/1, Gi0/2
     251 DVLAN0251                     DYNAMIC   Gi0/1
     252 VLAN0252                      STATIC    Gi0/1
```

(5) After the GVRP function is enabled globally, check whether user network devices dynamically create VLANs of user network. It indicates that the GVRP packets of user network are transmitted through the tunnels of SP devices.

Dynamic VLANs 70 to 79 have been created on CE 1, and the trunk port Gigabit Ethernet 0/2 joins the dynamic VLANs 70 to 79.

```
CE1(config)# show vlan
VLAN      Name                          Status    Ports
---------- -------------------------------- ---------
-----------------------------------
       1 VLAN0001                      STATIC    Gi0/1,Gi0/2, Gi0/3, Gi0/4
                                              Gi0/5, Gi0/6, Gi0/7, Gi0/8
    60-69 VLAN0060-VLAN0069              STATIC    Gi0/2
    70-79 DVLAN0070-DVLAN0079            DYNAMIC   Gi0/2
```

Dynamic VLANs 60 to 69 have been created on CE 2, and the trunk port Gigabit Ethernet 0/1 joins the dynamic VLANs 60 to 69.

```
CE2(config)# show vlan
VLAN      Name                          Status    Ports
---------- -------------------------------- ---------
-----------------------------------
       1 VLAN0001                      STATIC    Gi0/1,Gi0/2, Gi0/3, Gi0/4
                                              Gi0/5, Gi0/6, Gi0/7, Gi0/8
    60-69 DVLAN0060-DVLAN0069            DYNAMIC   Gi0/1
    70-79 VLAN0070-VLAN0079              STATIC    Gi0/1
```

6. Configuration Files

- PE 1 configuration file

```
l2protocol-tunnel gvrp
gvrp enable
gvrp dynamic-vlan-creation enable
!
vlan range 1,250-251
!
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 250
 switchport dot1q-tunnel native vlan 250
 l2protocol-tunnel gvrp enable
!
```

```
interface GigabitEthernet 0/2
 switchport mode trunk
```

- PE 2 configuration file

```
l2protocol-tunnel gvrp
gvrp enable
gvrp dynamic-vlan-creation enable
!
vlan range 1,250,252
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 250
 switchport dot1q-tunnel native vlan 250
 l2protocol-tunnel gvrp enable
```

- CE 1 configuration file

```
gvrp enable
gvrp dynamic-vlan-creation enable
!
vlan range 1,60-69
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

- CE 2 configuration file

```
gvrp enable
gvrp dynamic-vlan-creation enable
!
vlan range 1,70-79
!
interface GigabitEthernet 0/1
 switchport mode trunk
```

7. Common Errors

On the SP network, the configured GVRP BPDU tunnel addresses are inconsistent at two ends, causing that GVRP BPDU frames cannot be correctly transmitted.

Contents

1 Configuring QinQ....1
1.1 Introduction....1
1.1.1 Overview....1
1.1.2 Background and Function....1
1.1.3 QinQ Packet Format....1
1.1.4 QinQ Packet Forwarding....2
1.1.5 Basic QinQ Encapsulation....3
1.1.6 Selective QinQ Encapsulation....4
1.1.7 Modifying QinQ Tag....4
1.1.8 Layer-2 Protocol Tunneling....4
1.1.9 Protocols and Standards....5
1.2 Restrictions and Guidelines....5
1.3 Configuration Task Summary....6
1.3.1 Configuring Tag Adding....6
1.3.2 Configuring Layer-2 Protocol Tunneling....6
1.4 Configuring Basic QinQ Encapsulation....6
1.4.1 Overview....6
1.4.2 Restrictions and Guidelines....6
1.4.3 Procedure....7
1.5 Configuring C-Tag-Based Selective QinQ Encapsulation....7
1.5.1 Overview....7
1.5.2 Restrictions and Guidelines....7

1.5.3 Procedure....8

1.6 Configuring Priority Replication or Priority Mapping....9

1.6.1 Overview....9

1.6.2 Restrictions and Guidelines....9

1.6.3 Configuration Tasks....9

1.6.4 Configuring Priority Replication....9

1.6.5 Configuring Priority Mapping....10

1.7 Configuring TPID....11

1.7.1 Overview....11

1.7.2 Restrictions and Guidelines....11

1.7.3 Procedure....12

1.8 Configuring Layer-2 Protocol Tunneling....12

1.8.1 Overview....12

1.8.2 Restrictions and Guidelines....12

1.8.3 Configuration Tasks....13

1.8.4 Configuring STP Packet Tunneling....13

1.8.5 Configuring GVRP Packet Tunneling....13

1.9 Monitoring....14

1.10 Configuration Examples....15

1.10.1 Configuring Basic QinQ to Implement Layer-2 VPN....15

1.10.2 Configuring C-Tag-Based Selective QinQ to Implement Layer-2 VPN and Service Flow Management....23

1.10.3 Configuring ACL-Based Selective QinQ to Implementing Layer-2 VPN and Service Flow Management....27

1.10.4 Configuring Layer-2 Protocol Tunneling Based on QinQ....30

1 Configuring QinQ

1.1 Introduction

1.1.1 Overview

When a client packet enters a provider edge (PE), the QinQ technology first encapsulates the packet with a public virtual local area network (VLAN) tag before transmitting the packet in the SP network. The private VLAN tag, if any, in the client packet is regarded as data. Then, the packet carries two VLAN tags to pass through the SP network.

1.1.2 Background and Function

1. Background

On a metropolitan area network (MAN), SPs need a large number of VLANs to isolate and identify clients so as to achieve refined management. As a variety of services develop, SPs also need to differentiate services to provide different transmission pipelines and QoS policies. However, IEEE 802.1Q supports 4094 VLANs only, far from meeting the needs of SPs.

2. Function

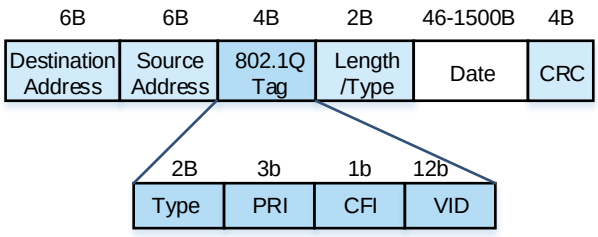
- QinQ is a kind of dual-tag encapsulation technology. It adds outer VLAN tags to packets in the SP network so that client VLANs in different private networks can be reused to increase the number of VLAN tags available to clients. The number of VLANs actually available to SPs is increased to 4094x4094.
- An outer tag is also equivalent to a tunnel, which enables transparent transmission of inner tags. This turns QinQ into a layer-2 VPN solution that is low in cost, easy to deploy, and suitable for small-sized networks.
- Inner and outer tags can also represent different information according to service requirements, helpful for SPs to segment and manage their services.

1.1.3 QinQ Packet Format

- Ethernet frame with a single VLAN tag

The IEEE 802.1Q standard modifies the Ethernet frame format by adding a 4-byte 802.1Q tag between the source MAC address field and protocol type field. Figure 1-1 shows the frame format. The tag contains a VID (VLAN ID) field, which is used to indicate the VLAN where the frame is. Not all devices can identify 802.1Q frames with tags, and therefore Ethernet frames on VLANs can be tagged or untagged.

Figure 1-1 Frame Format of 802.1Q Encapsulation

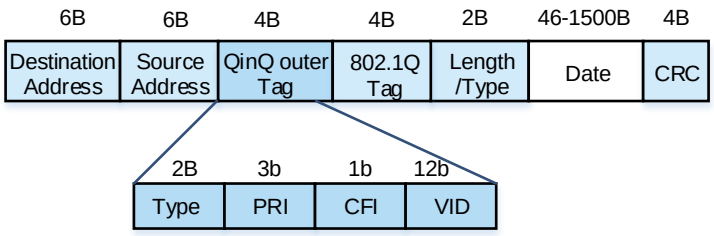


- **Type**: Consisting of 2 bytes; 0x8100 indicates 802.1Q frame. Devices that do not support IEEE 802.1Q will drop such frames received.
- **PRI**: Consisting of 3 bits, indicating layer-2 priority. The value range is 0 to 7, corresponding to CoS priorities of QoS. A larger value indicates a higher priority.
- **CFI**: Consisting of 1 bit, used to distinguish Ethernet frame, FDDI frame, and token ring network frame; 0 indicates Ethernet frame.
- **VID**: Consisting of 12 bits, indicating the client VLAN ID; values 0 and 4095 are reserved and unavailable. The value range is from 1 to 4094.

- Ethernet frame with QinQ dual VLAN tags

The QinQ function inserts a 4-byte QinQ outer tag (including four fields: **Type**, **PRI**, **CFI**, and **VID**) before the 802.1Q tag.

Figure 1-2 Frame Format of QinQ Encapsulation



- **Type**: Consisting of 2 bytes, also known as TPID; the default value is 0x8100, indicating 802.1Q frame. On the devices of some vendors, the TPID is set to 0x9100 or other values. TPID can be configured (Configuring TPID) to ensure that the TPIDs of packets to be forwarded are compatible with the TPIDs supported by third-party devices.
- **PRI**: Consisting of 3 bits, indicating priority; the default value 0 indicates a normal flow. The value of this field corresponds to the CoS value in the QoS policy. A larger value indicates a higher priority. The value of this field can be modified by configuring priority replication or priority mapping (Configuring Priority Replication or Priority Mapping) to define different transmission priority policies for packets.
- **CFI**: Consisting of 1 bit, used to distinguish Ethernet frame, FDDI frame, and token ring network frame; value 0 indicates Ethernet frame.
- **VID**: Consisting of 12 bits, indicating the SP VLAN ID. The value is from 1 to 4094.

1.1.4 QinQ Packet Forwarding

1. QinQ Encapsulation

The ingress of an SP's QinQ edge device is called dot1q-tunnel port, or tunnel port for short. All the frames entering the edge device, no matter whether they carry the 802.1Q tag or not, will be packaged with the SP tag and then be forwarded. As shown in Figure 1-3, when a packet of CE-A1 is forwarded to PE 1, the tunnel port encapsulates the packet with a VLAN 10 tag, and then forwards the packet from the uplink port. This process is called QinQ encapsulation. QinQ encapsulation is classified into Basic QinQ Encapsulation and Selective QinQ Encapsulation. Selective QinQ encapsulation is further classified into client tag-based encapsulation and ACL-based encapsulation.

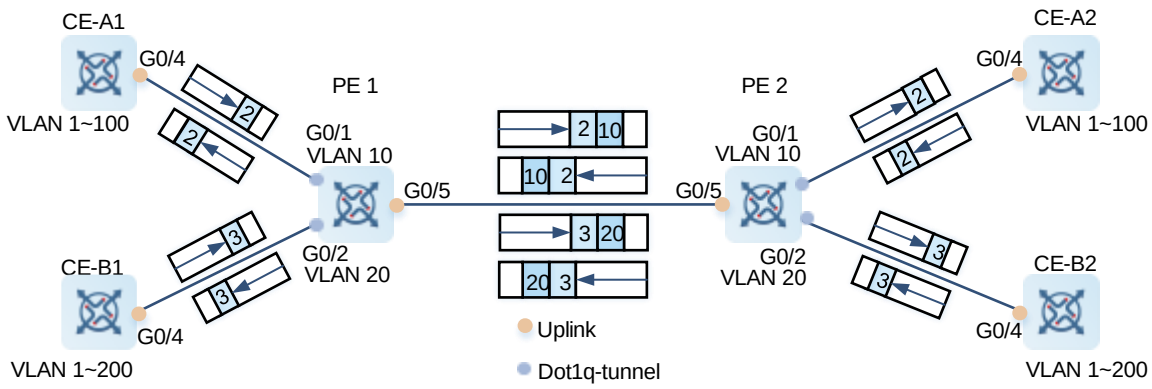
2. QinQ Forwarding

A QinQ-encapsulated packet will be transmitted in the SP network. Generally, devices directly forward the QinQ packet with dual tags. During the transmission, you may need to modify the VIDs in the inner and outer tags. In this case, you can configure a modification policy on the access, trunk, hybrid, or uplink port to modify QinQ tags (Modifying QinQ Tag).

3. QinQ Decapsulation

When a packet with an SP tag is forwarded to PE 2, PE 2 will forward the packet to the tunnel port with native VLAN set to VLAN 10, and the tunnel port will strip the outer tag of the packet and send the packet to CE-A2. This process is called QinQ decapsulation, and the decapsulation mode must be consistent with the encapsulation mode.

Figure 1-3 QinQ Packet Forwarding Process



Note

- The QinQ encapsulation and decapsulation functions are usually used on client-oriented interfaces to implement classification, package management, and transmission of client data.
- QinQ termination means that, after receiving packets, the device identifies and strips the dual VLAN tags, and then sends the packets to other service modules for processing. The QinQ termination function is usually used on a server or network core device to terminate client VLAN tags and realize the functions such as client location or service identification. QinQ termination is not QinQ decapsulation. QinQ decapsulation strips only the outer tag, while QinQ termination strips the dual tags.

1.1.5 Basic QinQ Encapsulation

The basic QinQ encapsulation mode is based on the process that the interface encapsulates the packets with tags. The VLAN ID in the tag is the native VLAN of dot1q-tunnel port.

After receiving packets, the dot1q-tunnel port regards all the packets as untagged regardless of whether they carry tags, determines whether the packets belong to the native VLAN of the local interface, learns the corresponding relationship between the client-end MAC address and the native VLAN, and stores it in the MAC address table. After that, the interface adds a tag with VID set to the native VLAN to the packets and then forwards the packets.

If the original packet does not carry a VLAN tag, the packet will have only one tag with native VLAN ID after undergoing QinQ encapsulation. If the original packet carries a VLAN tag, the packet will carry dual tags after undergoing QinQ encapsulation and be transmitted in the SP network.

By default, the native VLAN of dot1q-tunnel port is VLAN 1 and the only one allowed VLAN is untagged VLAN 1. "Untagged" in the QinQ function means that the outer tag of QinQ is not carried, because the dot1q-tunnel port must strip the outer tag before sending the packet back to the client network.

Weaknesses: The basic QinQ encapsulation cannot distinguish the types of client packets received by the interface or select the VLAN used for packet encapsulation, and therefore it is not flexible enough.

1.1.6 Selective QinQ Encapsulation

Selective QinQ encapsulation flexibly adds different outer VLAN tags to data flows according to rules.

Selective QinQ implements two encapsulation modes:

- Add an outer VLAN tag based on the inner client VLAN tag.

  The selective QinQ based on C-Tag can distinguish different types of data flows according to the client VLAN tag, and encapsulate different outer tags to implement transparent transmission.

- Add an outer VLAN tag based on the ACL.

  The selective QinQ based on ACL can distinguish the MAC address, IP protocol, source address, destination address, and priority of service flows, or the interface number of applications by using ACL policies, and encapsulate different service flows with different VLAN tags to implement transparent transmission. In this case, the VLAN ID in the VLAN tag is not necessarily the native VLAN of the interface.

When using this function, in addition to configuring the selective QinQ encapsulation policy, you also need to add the outer VLAN to the list of allowed VLANs of the dot1q-tunnel port.

Weaknesses: After the dot1q-tunnel port receives a packet, the learned MAC address entry is the corresponding relationship between the native VLAN and the client MAC address; the packet returned by the peer end belongs to the outer VLAN, and the corresponding entries of the outer VLAN and the client-end MAC address cannot be found in the MAC address table, which will cause the device to perform flooding so as to find the egress of packets.

1.1.7 Modifying QinQ Tag

In the process of QinQ packet transmission, if the outer or inner tags of data packets in the SP network need to be modified due to the actual network topology requirement, the QinQ tag modifying function needs to be enabled. The device can distinguish the packets of different clients, different services, and different priorities based on policies, and modify the VLAN IDs for the inner or outer tags of packets.

1.1.8 Layer-2 Protocol Tunneling

- Source

Spanning Tree Protocol (STP) is an application that eliminates layer-2 loops by blocking redundant links on the network. It also provides the link backup function. It will transmit a special bridge protocol data unit (BPDU) packet on the network. After recognizing such a packet, the device will calculate the spanning tree according to the packet information, which may lead to modification of the network topology.

The generic attribute registration protocol VLAN registration protocol (GVRP) is an application used to dynamically configure and diffuse VLAN memberships. It will transmit special VLAN registration and deregistration packets on the network. After recognizing a GVRP packet, the device will modify the VLAN relationship according to the packet information, which will also affect the network topology.

To unify the internal topology of the client network when the client networks are interconnected across the SP network, we need to run STP and GVRP on the client network. However, such a special layer-2 protocol packet will be identified as a special packet by the SP device and participate in the SP topology calculation, affecting the SP network topology.

Therefore, we need to transmit the STP and GVRP packets of the client network through a tunnel in the SP network, so that the SP can forward the client's special packets as ordinary packets. The layer-2 packet tunnel function is needed in this case.

- Principles

When a layer-2 protocol packet of the client network enters a PE, the destination MAC address is changed to a private address for forwarding in the SP network. When the packet arrives at an edge device of the other end, the destination MAC address is changed to a public address before the packet is returned to the client network of the other end. This implements layer-2 protocol packet transmission through a tunnel in the SP network.

1.1.9 Protocols and Standards

- IEEE 802.1ad: IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks---Amendment 4:Provider Bridges

1.2 Restrictions and Guidelines

- A routed port cannot be configured as a tunnel port. The **switchport** command can be used to configure an interface as a switch port.
- The IEEE 802.1x function cannot be enabled on an interface set to **Tunnel**.
- The port security function cannot be enabled on an interface set to **Tunnel**.
- When a tunnel port is configured as the source port of the remote switched port analyzer (RSPAN), the packets whose outer tags contain VIDs consistent with the RSPAN VLAN IDs are monitored as a data flow.
- If you want to match the ACL applied to the tunnel port with the VID in the client tag, use the **inner** keyword.
- After a switch port is enabled with QinQ, you must enable SVGL sharing before IGMP snooping. Otherwise, IGMP snooping will not work on the QinQ-enabled port. Please see *Configuring IGMP Snooping*.
- Configure the egress on the client network that is connected to the SP network as an uplink port. The SP TPID value for the uplink port of the client network must be the same as that for the downlink interface of the SP network.
- The default MTU value of an interface is 1,500 bytes. After added with an outer VLAN tag, a packet is four bytes longer. You are advised to increase the MTU value of each interface in the SP networks to at least 1,504 bytes.

1.3 Configuration Task Summary

1.3.1 Configuring Tag Adding

QinQ tag adding includes the following tasks:

(1) Configure the QinQ encapsulation mode of the tunnel port. Select at least one of them to configure.

- Configuring Basic QinQ Encapsulation
- Configuring C-Tag-Based Selective QinQ Encapsulation

(2) (Optional) Configuring Priority Replication or Priority Mapping. The following configuration tasks are mutually exclusive.

- Configuring Priority Replication
- Configuring Priority Mapping

(3) (Optional) Configuring TPID

1.3.2 Configuring Layer-2 Protocol Tunneling

The following tasks are optional.

- Configuring Layer-2 Protocol Tunneling. The following configuration tasks are optional.
  - Configuring STP Packet Tunneling
  - Configuring GVRP Packet Tunneling

1.4 Configuring Basic QinQ Encapsulation

1.4.1 Overview

Implement layer-2 VPN based on a port-based QinQ policy.

1.4.2 Restrictions and Guidelines

- Configure a VLAN of the SP network as the native VLAN of the dot1q-tunnel port. Because the trunk port will strip the tag of the packet whose VLAN ID is its native VLAN, do not configure the native VLAN of the trunk port in the SP network as the native VLAN of the dot1q-tunnel port.
- After the native VLAN of the dot1q-tunnel port is configured, the data of the VLAN cannot pass through the interface. The native VLAN must be added to the list of untagged VLANs allowed by the dot1q-tunnel port. After the configuration, the dot1q-tunnel port can output the packets of native VLAN without tags.
- If the native VLAN is added to the list of allowed tagged VLANs, packets of the native VLAN output from the dot1q-tunnel port will carry the tag of the SP VLAN, while the client device cannot identify the VLAN ID of SP network. Therefore, in order to ensure normal communication of the uplink and downlink packets in the application of QinQ, the SP VLAN (native VLAN) must be added to the allowed VLAN list of the interface in the untagged form.
- If port-based QinQ is enabled, you do not need to add the VLAN of the client network to the allowed VLAN list of the dot1q-tunnel port. If selective QinQ is enabled, add the VLAN of the client network to the allowed VLAN list of the interface in the tagged or untagged form based on the actual conditions.

1.4.3 Procedure

(1) Create an SP VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create an SP VLAN.

vlan *svid*

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the dot1q-tunnel port and allow SP VLAN packets to pass through.

a Enter the interface configuration mode of the port connected to the client network.

interface *interface-type interface-number*

b Configure the port as a dot1q-tunnel port.

switchport mode dot1q-tunnel

An interface works in access mode by default.

c Configure to add the SP VLAN to the untagged VLAN list of the dot1q-tunnel port.

switchport dot1q-tunnel allowed vlan { [**add**] **untagged** *svid* | **remove** *other-vlan-id* }

By default, the allowed VLAN of dot1q-tunnel port is untagged VLAN 1.

(3) Configure the SP VLAN as the native VLAN of dot1q-tunnel port so that the client network data is transmitted through a tunnel on the SP VLAN.

switchport dot1q-tunnel native vlan *svid*

The native VLAN of the dot1q-tunnel port is VLAN 1 by default.

1.5 Configuring C-Tag-Based Selective QinQ Encapsulation

1.5.1 Overview

Encapsulate outer VLAN tags (S-Tags) in packets based on inner tags to ensure preferential transmission and management of layer-2 VPN and service flows.

1.5.2 Restrictions and Guidelines

- This function must be configured based on the basic QinQ, and prevails over the basic QinQ policy.
- In the network environment, for packets received on the dot1q-tunnel port, the VID of the outer tag needs to be modified according to the VID of the inner tag. With this command, you can add an outer VID the same as the inner VID to the packet so as to output the original VID tag packet from the egress.
- To continue to adopt the VLAN tag priority specified by the client network, you can configure priority replication to configure an outer tag the same as the inner tag.

- If the SP network requires the transmission of packets based on the priority of the outer tag, you also need to configure priority replication to set the CoS of the outer tag to the specified value.

Caution

- The priority of the VID change policies in a descending order: ACL-based > C-Tag-based > port-based.
- When a member is added to/deleted from an aggregation port, the policy of adding or modifying the VID configured on the aggregation port is deleted and needs to be reconfigured. You are advised to configure the VIP policy on an aggregation port after configuring the members.
- You must configure the tunnel port and the interface connected to the public network to permit packets with specified VLAN IDs (including the native VLAN ID) in the outer tag to pass through.

1.5.3 Procedure

(1) Create an SP VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a group of SP VLANs.

vlan range *svidA,svidB*

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the dot1q-tunnel port and allow SP VLAN packets to pass through.

a Enter the interface configuration mode of the port connected to the client network.

interface *interface-type interface-number*

b Configure the port as a dot1q-tunnel port.

switchport mode dot1q-tunnel

An interface works in access mode by default.

c Configure to add the SP VLAN to the untagged VLAN list of the dot1q-tunnel port.

switchport dot1q-tunnel allowed vlan { [**add**] **untagged** *svidA,svidB* | **remove** *other-vlan-id* }

By default, the allowed VLAN of dot1q-tunnel port is untagged VLAN 1.

(3) Configure the C-Tag-based QinQ encapsulation rule. The packets of different client VLANs are allocated to different SP VLANs for transmission through a tunnel.

a The packets of client VLAN *cvid-lista* are allocated to the SP VLAN *svidA*.

dot1q outer-vid *svidA* **register inner-vid** *cvid-lista*

No policy of adding an outer VID based on the inner VID of packets is configured by default.

b The packets of client VLAN *cvid-listb* are allocated to the SP VLAN *svidB*.

dot1q outer-vid *svidB* **register inner-vid** *cvid-listb*

No policy of adding the outer VID based on the inner VID of packets is configured by default.

1.6 Configuring Priority Replication or Priority Mapping

1.6.1 Overview

This function configures the CoS value of the outer tag based on the user priority value (CoS) of the client VLAN tag by replication or mapping.

- Priority replication

By default, the user priority (PRI) field of the Ethernet frame tag is 0, namely, the normal flow. To make the specified packet preferentially processed and transmitted, configure this field to change the priority of the packet. The value of this field corresponds to the CoS value in the QoS policy. The CoS-based QoS policy can be configured to ensure the processing priority of a service.

If the VLAN tag of a client packet is configured with the CoS value of the user priority, and the QoS priority policy is configured in the SP network for the CoS value, the CoS value for the VLAN tag of client packet can be replicated as the CoS value of the outer tag, so that the client packet can be transmitted transparently and the QoS priority policy provided by the SP network can be used.

- Priority mapping

When an outer VLAN tag is added, the user priority of the outer VLAN tag can be set according to the user priority of the inner VLAN tag through priority mapping so that the network QoS priority policy can be used after the packet is encapsulated with an outer VLAN tag.

The SP network sets different QoS policies for multiple CoS values, corresponding to different service flow services. To make some client services be preferentially transmitted in the SP network, the priority mapping function can be configured. The CoS value of the outer VLAN tag can be specified according to the CoS value of the client inner VLAN tag, so that the packet can enjoy the QoS policy of the SP network after being encapsulated with the outer VLAN tag.

1.6.2 Restrictions and Guidelines

- Priority replication and priority mapping cannot be enabled on the same interface at the same time.
- Priority replication or priority mapping of client tags can be configured only on the dot1q-tunnel port.

1.6.3 Configuration Tasks

The following configuration tasks are mutually exclusive. Select one task.

- Configuring Priority Replication
- Configuring Priority Mapping

1.6.4 Configuring Priority Replication

1. Overview

It is assumed that the SP network is configured with the QoS policy based on the user priority value (CoS) of client VLAN tag. If the CoS value of an inner tag is 3, the CoS value of the outer tag can be set to 3 by configuring priority replication, so that the packet can enjoy the QoS policy with a priority of 3 as the inner tag after being encapsulated with the outer VLAN tag.

Configure priority replication to apply the QoS policy provided by the SP network for the client VLAN tag.

2. Restrictions and Guidelines

Priority replication has a higher priority than trusted QoS but lower than ACL data flow-based QoS.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the CoS priority for trusted packets of the interface.

mls qos trust cos

The default trust mode of an interface is untrust.

(5) Configure priority replication.

inner-priority-trust enable

The priority replication function is disabled by default.

1.6.5 Configuring Priority Mapping

1. Overview

It is assumed that the SP network is set with the QoS policy based on the user priority value (CoS) of client VLAN tag. Suppose the CoS value of an inner tag is 3. The CoS value of the outer tag can be set to 5 by configuring priority mapping (CoS-to-CoS), so that the packet can enjoy the QoS policy with a priority of 5 after being encapsulated with the outer VLAN tag.

If the user priority of the outer VLAN tag needs to be set according to the VLAN tag of the client to flexibly apply the QoS priority, configure the priority mapping policy.

2. Restrictions and Guidelines

- Priority mapping takes precedence over QoS.
- If no trust mode is configured (namely, **Trust None**) or the configured trust mode is not matched with priority mapping, the configuration of priority mapping does not take effect.
- If no priority mapping is configured, the following mapping is used by default, and the value ranges of *inner-cos-value* and *outer-cos-value* are from 0 to 7.

Table 1-1 Default Priority Mapping

Inner CoS	0	1	2	3	4	5	6	7
Outer CoS	0	1	2	3	4	5	6	7

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the CoS priority for trusted packets of the interface.

mls qos trust cos

The default trust mode of an interface is untrust.

(5) (Optional) Disable priority replication.

no inner-priority-trust enable

The priority replication function is disabled by default.

(6) Configure priority mapping.

dot1q-tunnel cos *inner-cos-value* **remark-cos** *outer-cos-value*

No priority mapping rule is set by default.

1.7 Configuring TPID

1.7.1 Overview

An Ethernet frame tag consists of four fields: Tag Protocol Identifier (**TPID**, written as **Type** in the frame format map), User Priority (**PRI**), **CFI**, and **VLAN ID**.

The TPID value is 0x8100 by default, while the devices of some vendors set the TPID value for the outer tag of packets to 0x9100 or other values. To be compatible with these devices, this device supports port-based TPID modification for packets.

You can configure the TPID value of ports independently. When forwarding packets, these ports replace the TPID in the outer VLAN tag of the packets with the value set by the user, ensuring compatibility with the TPIDs of different vendors.

Purpose: The interface on the PE that connects to the public network needs to be configured as an uplink port. Configure the TPIDs in the tags on SP network devices to realize TPID compatibility with third-party devices. Perform the configuration in interface configuration mode of the uplink port.

1.7.2 Restrictions and Guidelines

- If a PE is connected to a third-party device on which the TPID is not the default value 0x8100 of IEEE 802.1Q, you need to configure the TPID on the interface connected to the third-party device.

Caution

Do not set the TPID to the following well-known types: 0x0806 (ARP), 0x0200 (PUP), 0x8035 (RARP), 0x0800 (IP), 0x86DD (IPv6), 0x8863/0x8864 (PPPoE), 0x8847/0x8848 (MPLS), 0x8137 (IPX/SPX), 0x8000 (IS-IS), 0x8809 (LACP), 0x888E (802.1x), 0x88A7 (cluster), and 0x0789 (reserved).

- TPIDs can be configured in interface configuration mode and global configuration mode.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode of the port of the PE that is connected to the public network.

interface *interface-type interface-number*

(4) Configure this port as an uplink port.

switchport mode uplink

An interface works in access mode by default.

(5) Configure the TPID value.

frame-tag tpid *tpid*

The TPID value is 0x8100 by default.

1.8 Configuring Layer-2 Protocol Tunneling

1.8.1 Overview

BPDU tunneling is a layer-2 tunneling function based on the Layer 2 Tunnel Protocol (L2TP).

When the tunnel port of a PE receives STP BPDU packets from the client network, due to their special destination MAC address, the PE will not process them as ordinary client packets, but will recognize them as BPDU packets and not forward them. It will also calculate the spanning tree according to the content of BPDU. This may affect the topology of the SP network. Similarly, when the tunnel interlace of a PE receives GVRP BPDU packets from the client network, the PE will not forward them, but will update the VLAN information according to the packet content. This may affect the topology of the SP network.

When the STP or GVRP function is also enabled for the SP device, the BPDU tunnel function needs to be used to transmit the STP and GVRP packets of the client network in the SP network without affecting the SP network.

When the BPDU packets on the client network enter the tunnel port of the PE, the destination MAC address is changed to the private address and then the packets are forwarded in the SP network. When the packets reach the PE at the other end, the destination MAC address is changed to the public address and the packets are transmitted on the client network at the other end. This achieves transmission of the BPDU packets through the tunnel in the SP network, preventing the client network and the SP network from interfering with each other.

1.8.2 Restrictions and Guidelines

- If STP or GVRP is not enabled for the SP device, you can configure **bridge-frame forwarding protocol bpdu** to enable transparent transmission of BPDU packets.
- To make protocol tunneling effective on an interface, you need to first enable protocol tunneling in global configuration mode. When the protocol tunneling function on an interface takes effect, the interface does not participate in protocol calculation. If the tunnel port receives a packet whose destination MAC address is a special multicast address, there is an error in the networking and the packet will be dropped directly.

1.8.3 Configuration Tasks

The configuration includes the following tasks:

- Configuring STP Packet Tunneling
- Configuring GVRP Packet Tunneling

1.8.4 Configuring STP Packet Tunneling

1. Overview

If the STP function is enabled for the SP device and STP BPDU packets of the client network need to be transmitted, this function must be configured.

2. Restrictions and Guidelines

- The STP tunneling function takes effect only when it is enabled in global configuration mode and interface configuration mode respectively.
- The optional tunnel addresses of STP packets are 01d0.f800.0005 (default value), 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the STP tunneling function globally.

l2protocol-tunnel stp

The STP packet tunneling function is disabled by default.

(4) (Optional) Configure a tunnel address in the corresponding protocol.

l2protocol-tunnel stp tunnel-dmac *mac-address*

The STP packet tunnel address is 01d0.f800.0005 by default.

(5) Enter the interface configuration mode.

interface *interface-type interface-number*

(6) Enable the STP tunneling function on the interface.

l2protocol-tunnel stp enable

The STP packet tunneling function is disabled for the dot1q-tunnel port by default.

1.8.5 Configuring GVRP Packet Tunneling

1. Overview

If the GVRP function is enabled for the SP device and GVRP BPDU packets of the client network need to be transmitted, this function must be configured.

2. Restrictions and Guidelines

- The GVRP tunneling function takes effect only when it is enabled in global configuration mode and interface

configuration mode respectively.

- The optional tunnel addresses of GVRP packets are 01d0.f800.0006 (default value) and 011a.a900.0006.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the GVRP tunneling function globally.

l2protocol-tunnel gvrp

The GVRP packet tunneling function is disabled by default.

(4) (Optional) Configure a tunnel address in the corresponding protocol.

l2protocol-tunnel gvrp tunnel-dmac *mac-address*

The GVRP packet tunnel address is 01d0.f800.0006 by default.

(5) Enter the interface configuration mode.

interface *interface-type interface-number*

(6) Enable the GVRP tunneling function on the interface.

l2protocol-tunnel gvrp enable

The GVRP packet tunneling function is disabled for the dot1q-tunnel port by default.

1.9 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

This section also describes the **debug** command used for outputting debugging information.

Caution

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

You can run the **clear** commands to clear information.

Caution

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

Table 1-2 Monitoring

Command	Purpose
show dot1q-tunnel [**interfaces** *interface-type interface-number*]	Displays whether the dot1q-tunnel function is enabled on the interface.
show interfaces dot1q-tunnel	Displays configuration of the dot1q-tunnel port.

Command	Purpose
show registration-table [**interfaces** *interface-type interface-number*]	Displays the policy of adding the VID based on the protocol on the dot1q-tunnel port.
show translation-table [**interfaces** *interface-type interface-number*]	Displays the policy of modifying the VID based on the access, trunk, and hybrid ports.
show frame-tag tpid interfaces [*interface-type interface-number*]	Displays the TPID configuration of the interface.
show inner-priority-trust [**interfaces** *interface-type interface-number*]	Displays the configuration of priority replication.
show interfaces [*interface-type interface-number*] **remark**	Displays the configuration of priority mapping.
show l2protocol-tunnel { **gvrp** | **stp** }	Displays the layer-2 tunnel configuration.
debug bridge qinq	Enables the QinQ debugging function.

1.10 Configuration Examples

1.10.1 Configuring Basic QinQ to Implement Layer-2 VPN

1. Requirements

An SP provides a VPN for Company A and Company B, as shown in Figure 1-4. Basic QinQ is enabled on PEs to meet the layer-2 VPN requirement. On the public network, Company A and Company B belong to different VLANs, and client data packets are transmitted on different native VLANs to implement the simple layer-2 VPN.

- Company A uses public VLAN 10. In Area 1, clients are connected through CE-A1 and access the public network through PE 1; in Area 2, clients are connected through CE-A2, and access the public network through PE 2. The tunnel port first encapsulates the client data packets of Company B with one VLAN 10 tag, and then forwards them on the public network.
- Company B uses public VLAN 20. In Area 1, clients are connected through CE-B1 and access the public network through PE 1; in Area 2, clients are connected through CE-B2, and access the public network through PE 2. The tunnel port first encapsulates the client data packets of Company B with one VLAN 20 tag, and then forwards them on the public network.

The client VLANs in Company A and Company B are transparent to the public network. The client VLANs can be reused without conflicts. Therefore, client VLANs do not need to be configured on the SP device, but need to be configured only on the CE device.

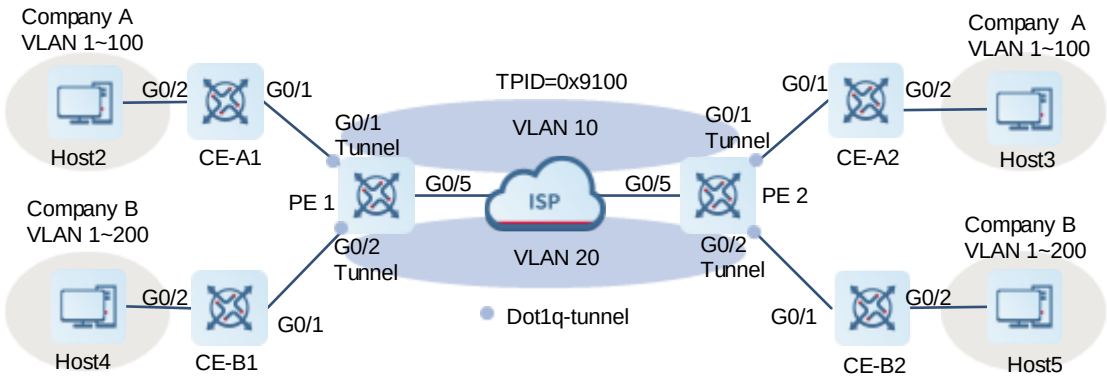
- The office network VLAN of Company A ranges from 1 to 100.
- The office network VLAN of Company B ranges from 1 to 200.

The priority replication and priority mapping functions of CoS can be configured on the tunnel port of the PE, and the QoS policy of CoS is configured to enable the client data packets to enjoy different QoS policies.

Generally, the TPID of the device is 0x8100 specified in IEEE 802.1Q. Because there are some devices in the SP network whose TPID is 0x9100, the TPID value needs to be modified on the uplink port of PE to ensure compatibility with these devices.

2. Topology

Figure 1-4 Basic QinQ Implements Layer-2 VPN



3. Notes

- Configure the interfaces on PE 1 and PE 2 connected to CE-A1, CE-A2, CE-B1 and CE-B2 as tunnel ports. The public network transmission VLAN is the native VLAN of the tunnel port, and belongs to the allowed untagged VLAN list of the port.
- Configure the interface on the PE that connects to the public network as a trunk, hybrid, or uplink port. When the connection interface between SP devices is a trunk or hybrid port, do not configure the native VLAN of the trunk or hybrid port as the native VLAN of dot1q-tunnel port. The reason is that, when the packets of the native VLAN is output from the trunk or hybrid port, the interface will strip the tag from the packet.
- The client VLAN is configured on the CE according to the user's needs, and the uplink port on the CE is configured as trunk, hybrid, or uplink port.

4. Procedure

(1) Configure the basic QinQ transmission channel VLAN 10 of Company A. VLAN 10 is the native VLAN of the tunnel port, and belongs to the allowed untagged VLAN list of the tunnel port.

On PE 1, configure VLAN 10 to implement tunnel transmission for the data of Company A's network.

```
PE1> enable
PE1# configure terminal
PE1(config)# vlan 10
PE1(config-vlan)# exit
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-GigabitEthernet 0/1)# switchport
PE1(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
PE1(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel native vlan 10
PE1(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan add
untagged 10
PE1(config-if-GigabitEthernet 0/1)# exit
```

On PE 2, configure VLAN 10 to implement tunnel transmission for the data of Company A's network.

```
PE2> enable
PE2# configure terminal
PE2(config)# vlan 10
PE2(config-vlan)# exit
PE2(config)# interface gigabitethernet 0/1
PE2(config-if-GigabitEthernet 0/1)# switchport
PE2(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
PE2(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel native vlan 10
PE2(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan add
untagged 10
PE2(config-if-GigabitEthernet 0/1)# exit
```

(2) Configure the basic QinQ transmission channel VLAN 20 of Company B. VLAN 20 is the native VLAN of the tunnel port, and belongs to the allowed untagged VLAN list of the tunnel port.

On PE 1, configure VLAN 20 to implement tunnel transmission for the data of Company B's network.

```
PE1(config)# vlan 20
PE1(config-vlan)# exit
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-GigabitEthernet 0/2)# switchport
PE1(config-if-GigabitEthernet 0/2)# switchport mode dot1q-tunnel
PE1(config-if-GigabitEthernet 0/2)# switchport dot1q-tunnel native vlan 20
PE1(config-if-GigabitEthernet 0/2)# switchport dot1q-tunnel allowed vlan add
untagged 20
PE1(config-if-GigabitEthernet 0/2)# exit
```

On PE 2, configure VLAN 20 to implement tunnel transmission for the data of Company B's network.

```
PE2(config)# vlan 20
PE2(config-vlan)# exit
PE2(config)# interface gigabitethernet 0/2
PE2(config-if-GigabitEthernet 0/2)# switchport
PE2(config-if-GigabitEthernet 0/2)# switchport mode dot1q-tunnel
PE2(config-if-GigabitEthernet 0/2)# switchport dot1q-tunnel native vlan 20
PE2(config-if-GigabitEthernet 0/2)# switchport dot1q-tunnel allowed vlan add
untagged 20
PE2(config-if-GigabitEthernet 0/2)# exit
```

(3) Configure the interface on the PE for connecting to the public network as a trunk port. VLAN 10 and VLAN 20 need to be added to the allowed VLAN list of the trunk port, but cannot be the native VLAN of the trunk port.

Configure the interface on PE 1 for connecting to the public network as a trunk port, and modify the TPID value of output packets to 0x9100.

```
PE1(config)# interface gigabitethernet 0/5
PE1(config-if-GigabitEthernet 0/5)# switchport mode trunk
PE1(config-if-GigabitEthernet 0/5)# frame-tag tpid 9100
PE1(config-if-GigabitEthernet 0/5)# end
PE1# write
```

Configure the interface on PE 2 for connecting to the public network as a trunk port, and modify the TPID value of output packets to 0x9100.

```
PE2(config)# interface gigabitethernet 0/5
PE2(config-if-GigabitEthernet 0/5)# switchport mode trunk
PE2(config-if-GigabitEthernet 0/5)# frame-tag tpid 9100
PE2(config-if-GigabitEthernet 0/5)# end
PE2# write
```

(4) On the CE, configure the interface for connecting to the PE as a trunk port, and configure the interface for connecting to the user terminal as an access port and add it to the client VLAN.

Create client VLANs 1–100 on CE-A1; configure the interface GigabitEthernet 0/1 for connecting to the PE as a trunk port; configure one client interface GigabitEthernet 0/2 to join VLAN 60 (the configuration of other client interfaces is omitted here).

```
CE-A1> enable
CE-A1# configure terminal
CE-A1(config)# vlan range 1-100
CE-A1(config-vlan)# exit
CE-A1(config)# interface gigabitethernet 0/1
CE-A1(config-if-GigabitEthernet 0/1)# switchport
CE-A1(config-if-GigabitEthernet 0/1)# switchport mode trunk
CE-A1(config-if-GigabitEthernet 0/1)# exit
CE-A1(config)# interface gigabitethernet 0/2
CE-A1(config-if-GigabitEthernet 0/2)# switchport
CE-A1(config-if-GigabitEthernet 0/2)# switchport access vlan 60
```

Create client VLANs 1–100 on CE-A2; configure the interface GigabitEthernet 0/1 for connecting to the PE as a trunk port; configure one client interface GigabitEthernet 0/2 to join VLAN 60 (the configuration of other client interfaces is omitted here).

```
CE-A2> enable
CE-A2# configure terminal
CE-A2(config)# vlan range 1-100
CE-A2(config-vlan)# exit
CE-A2(config)# interface gigabitethernet 0/1
CE-A2(config-if-GigabitEthernet 0/1)# switchport
CE-A2(config-if-GigabitEthernet 0/1)# switchport mode trunk
CE-A2(config-if-GigabitEthernet 0/1)# exit
CE-A2(config)# interface gigabitethernet 0/2
CE-A2(config-if-GigabitEthernet 0/2)# switchport
CE-A2(config-if-GigabitEthernet 0/2)# switchport access vlan 60
```

Create client VLANs 1–200 on CE-B1; configure the interface GigabitEthernet 0/1 for connecting to the PE as a trunk port; configure one client interface GigabitEthernet 0/2 to join VLAN 60 (the configuration of other client interfaces is omitted here).

```
CE-B1> enable
CE-B1# configure terminal
CE-B1(config)# vlan range 1-200
CE-B1(config-vlan)# exit
```

```
CE-B1(config)# interface gigabitethernet 0/1
CE-B1(config-if-GigabitEthernet 0/1)# switchport
CE-B1(config-if-GigabitEthernet 0/1)# switchport mode trunk
CE-B1(config-if-GigabitEthernet 0/1)# exit
CE-B1(config)# interface gigabitethernet 0/2
CE-B1(config-if-GigabitEthernet 0/2)# switchport
CE-B1(config-if-GigabitEthernet 0/2)# switchport mode access
CE-B1(config-if-GigabitEthernet 0/2)# switchport access vlan 60
```

Create client VLANs 1–200 on CE-B2; configure the interface GigabitEthernet 0/1 for connecting to the PE as a trunk port; configure the client interface GigabitEthernet 0/2 to join VLAN 60 (the configuration of other client interfaces is omitted here).

```
CE-B2> enable
CE-B2# configure terminal
CE-B2(config)# vlan range 1-200
CE-B2(config-vlan)# exit
CE-B2(config)# interface gigabitethernet 0/1
CE-B2(config-if-GigabitEthernet 0/1)# switchport
CE-B2(config-if-GigabitEthernet 0/1)# switchport mode trunk
CE-B2(config-if-GigabitEthernet 0/1)# exit
CE-B2(config)# interface gigabitethernet 0/2
CE-B2(config-if-GigabitEthernet 0/2)# switchport
CE-B2(config-if-GigabitEthernet 0/2)# switchport mode access
CE-B2(config-if-GigabitEthernet 0/2)# switchport access vlan 60
```

5. Verification

(1) Display the interface configuration of PEs.

Display the interface configuration of PE 1.

```
PE1# show interfaces switchport
Interface                    Switchport Mode     Access Native Protected VLAN
lists
------------------------------- ---------- --------- ------ ------ ---------
----------------
GigabitEthernet 0/1            enabled   TUNNEL   1     10    Disabled  1,10
GigabitEthernet 0/2            enabled   TUNNEL   1     20    Disabled  1,20
GigabitEthernet 0/5            enabled   TRUNK    1     1     Disabled  ALL
```

Display the interface configuration of PE 2.

```
PE2# show interfaces switchport
Interface                    Switchport Mode     Access Native Protected VLAN
lists
------------------------------- ---------- --------- ------ ------ ---------
----------------
GigabitEthernet 0/1            enabled   TUNNEL   1     10    Disabled  1,10
GigabitEthernet 0/2            enabled   TUNNEL   1     20    Disabled  1,20
GigabitEthernet 0/5            enabled   TRUNK    1     1     Disabled  ALL
```

(2) Display the tunnel port configuration of PEs.

Display the tunnel port configuration of PE 1.

```
PE1# show interfaces dot1q-tunnel
========Interface Gi0/1========
Native vlan: 10
Allowed vlan list:1,10,
Tagged vlan list:
========Interface Gi0/2========
Native vlan: 20
Allowed vlan list:1,20,
Tagged vlan list:
```

Display the tunnel port configuration of PE 2.

```
PE2# show interfaces dot1q-tunnel
========Interface Gi0/1========
Native vlan: 10
Allowed vlan list:1,10,
Tagged vlan list:
========Interface Gi0/2========
Native vlan: 20
Allowed vlan list:1,20,
Tagged vlan list:
```

(3) Display the uplink port configuration of PEs.

Display the uplink port configuration of PE 1.

```
PE1# show frame-tag tpid
Ports        Tpid
------------  ----------
Gi0/5        0x9100
```

Display the uplink port configuration of PE 2.

```
PE2# show frame-tag tpid
Ports        Tpid
------------  ----------
Gi0/5        0x9100
```

(4) Display the CE configuration of Company A.

Display the configuration of CE-A1.

```
CE-A1(config)# show interface switchport
Interface                    Switchport Mode     Access Native Protected VLAN
lists
-------------------------------- ---------- --------- ------ ------ ---------
----------------
GigabitEthernet 0/1            enabled    TRUNK    1      1      Disabled  ALL
GigabitEthernet 0/2            enabled    ACCESS    60     1      Disabled  ALL
```

Display the configuration of CE-A2.

```
CE-A2(config)#show interface switchport
```

```
Interface                    Switchport Mode     Access Native Protected VLAN
lists
------------------------------- ---------- --------- ------ ------ ---------
----------------
GigabitEthernet 0/1            enabled   TRUNK    1     1     Disabled  ALL
GigabitEthernet 0/2            enabled   ACCESS   60    1     Disabled  ALL
```

(5) Take Hosts 2 and 3 as examples to verify that clients in Company A can implement layer-2 interworking.

Configure an IP address for Host 2.

```
Host2> enable
Host2# configure terminal
Host2(config)#interface gigabitethernet 0/1
Host2(config-if-GigabitEthernet 0/1)#no switchport
Host2(config-if-GigabitEthernet 0/1)#ip address 192.168.60.2/24
```

Configure an IP address for Host 3.

```
Host3> enable
Host3# configure terminal
Host3(config)#interface gigabitethernet 0/1
Host3(config-if-GigabitEthernet 0/1)#no switchport
Host3(config-if-GigabitEthernet 0/1)#ip address 192.168.60.3/24
```

Verify that Host 2 can ping through Host 3.

```
Host2# ping 192.168.60.3
Sending 5, 100-byte ICMP Echoes to 192.168.60.3, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/6 ms.
```

(6) Take Hosts 4 and 5 as examples to verify that clients in Company B can implement layer-2 interworking.

Configure an IP address for Host 4.

```
Host4> enable
Host4# configure terminal
Host4(config)#interface gigabitethernet 0/1
Host4(config-if-GigabitEthernet 0/1)#no switchport
Host4(config-if-GigabitEthernet 0/1)#ip address 192.168.60.4/24
```

Configure an IP address for Host 5.

```
Host5> enable
Host5# configure terminal
Host5(config)#interface gigabitethernet 0/1
Host5(config-if-GigabitEthernet 0/1)#no switchport
Host5(config-if-GigabitEthernet 0/1)#ip address 192.168.60.5/24
```

Verify that Host 4 can ping through Host 5.

```
Host4# ping 192.168.60.5
Sending 5, 100-byte ICMP Echoes to 192.168.60.5, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/6 ms.
```

(7) Host 2 in Company A cannot ping through Host 5 in Company B, which indicates that clients in different companies cannot implement layer-2 interworking.

```
Host2# ping 192.168.60.5
Sending 5, 100-byte ICMP Echoes to 192.168.60.5, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

6. Configuration Files

- Configuration files of PE 1 and PE 2

```
vlan range 1,10,20
!
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 10
 switchport dot1q-tunnel native vlan 10
!
interface GigabitEthernet 0/2
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 20
 switchport dot1q-tunnel native vlan 20
!
interface GigabitEthernet 0/5
 switchport mode trunk
 frame-tag tpid 0x9100
```

- Configuration files of CE-A1 and CE-A2 (Only GigabitEthernet 0/2 is taken as an example of interfaces connected to user terminals; the configuration files of the other interfaces are omitted.)

```
vlan range 1-100
!
interface gigabitethernet 0/1
switchport mode trunk
!
interface gigabitethernet 0/2
switchport access vlan 60
```

- Configuration files of CE-B1 and CE-B2 (Only GigabitEthernet 0/2 is taken as an example of interfaces connected to user terminals; the configuration files of the other interfaces are omitted.)

```
vlan range 1-200

interface gigabitethernet 0/1
switchport mode trunk

interface gigabitethernet 0/2
switchport access vlan 60
```

7. Common Errors

- The same company has different native VLANs on the dot1q-tunnel ports of PE 1 and PE 2, which leads to the failure of interworking.
- The native VLAN of the dot1q-tunnel is not added to the allowed VLAN list of the interface in the untagged form.
- The TPID value of a third-party device is not the default value 0x8100, but the TPID is not configured on the egress connected to the third-party device, and therefore the packet cannot be recognized by the third-party device.

1.10.2 Configuring C-Tag-Based Selective QinQ to Implement Layer-2 VPN and Service Flow Management

1. Requirements

Broadband Internet access and IPTV are important services carried by the metropolitan area network (MAN). MAN SPs allocate different service flows to different SP VLANs to achieve differentiated management, and provide QoS policy services for these VLANs or CoSs.

The basic QinQ function can encapsulate the client data packets received by the tunnel port only with the outer tag with the same VLAN ID, and the VLAN ID of outer tags is the native VLAN of the tunnel port; the basic QinQ cannot meet the requirement for differentiating SP VLANs in multi-service scenarios.

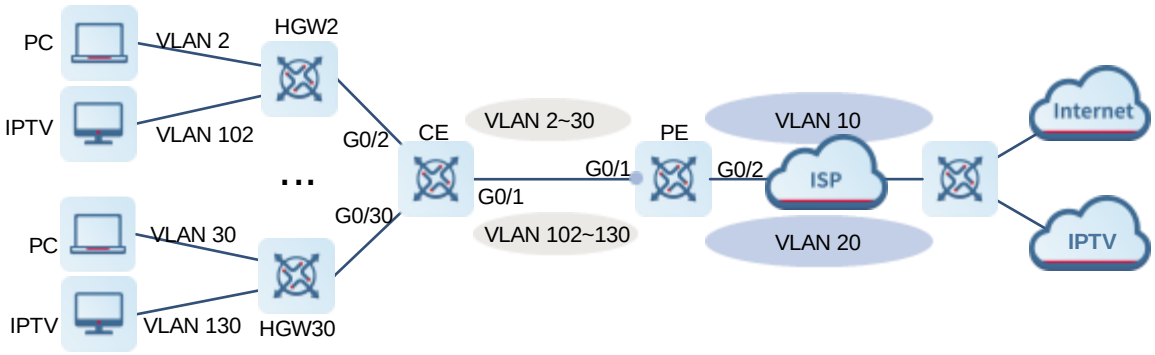
Selective QinQ can flexibly add the SP outer tag (S-Tag) according to the tag (C-Tag) of client packets, encapsulate the client service flows received by the same tunnel port into different SP VLANs, and use the QoS policy of SP network to guarantee reliability while transparently transmitting client data.

As shown in Figure 1-5, devices involved include provider edges (PEs), customer edges (CEs), and home gateways (HGWs) 1–30.

- The broadband Internet access data and IPTV service data are allocated to different VLANs. VLANs 2–30 are for client broadband Internet access service flows, and VLANs 102–130 are for client IPTV service flows.
- On the public network, the broadband Internet access data is transmitted through SP VLAN 10 to implement data communication with the Internet; the IPTV service flow is transmitted through VLAN 20 to implement data communication with the IPTV network. The tunnel port is configured on PE, and different VLANs are encapsulated to distinguish different service data. Client VLANs 2–30 are encapsulated as SP VLAN 10, while client VLANs 102–130 are encapsulated as SP VLAN 20.
- Client network packets carry tags and contain the CoS priority. The SP network enables the priority replication function on PEs, and uses the CoS value for the inner tag of packets in the outer tag so that service flows of the client network can use the QoS policy of the SP network to ensure transmission.

2. Topology

Figure 1-5 Selective QinQ Implements Layer-2 VPN



3. Notes

- Configure the interface GigabitEthernet 0/1 of PE for connecting to CE as tunnel port. Add SP VLANs 10 and 20 to the untagged VLAN list of the tunnel port connected to the client network so that the packets from the peer end return to the tunnel port and the SP tag is stripped when packet output.
- On the downlink interface of PE, configure the selective QinQ function of adding outer VLAN tags based on C-Tag. If the tunnel port receives the frames of client VLANs 2–30 (C-Tag), the frames will be encapsulated with the tag (S-Tag) of SP VLAN 10; if the tunnel port receives the frames of client VLANs 102–130 (C-Tag), the frames will be encapsulated with the tag (S-Tag) of SP VLAN 20.
- The SP network provides the CoS-based QoS priority policy. You can configure priority replication to replicate the CoS value of the client VLAN tag to the CoS of the outer VLAN tag so that the packet encapsulated with the outer tag is transmitted based on the priority policy for the client VLAN tag.
- The interface of PE for connecting to the public network is configured as an uplink port to transmit the data of VLAN 10 and VLAN 20.
- The interface of CE for connecting to the PE is configured as an uplink port to transmit the data of VLANs 2–30 and VLANs 102–130.
- The interface of CE for connecting to HGW is configured as a trunk port, and the VLAN transmitted by HGW device is added to the allowed VLAN list of the trunk port. The clients adopting HGW 2 use VLAN 2 to transmit broadband Internet access data and VLAN 102 to transmit IPTV data. The clients adopting HGW 30 use VLAN 30 to transmit broadband Internet access data and VLAN 130 to transmit IPTV data. The configurations of other clients are similar.

4. Procedure

(1) Configure the C-Tag-based QinQ encapsulation rule.

Add SP VLAN 10 and VLAN 20 to the untagged VLAN list of the tunnel port GigabitEthernet 0/1.

```
PE> enable
PE# configure terminal
PE(config)# vlan range 10,20
PE(config-vlan-range)# exit
PE(config)# interface gigabitethernet 0/1
```

```
PE(config-if-GigabitEthernet 0/1)# switchport
PE(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
PE(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan add
untagged 10,20
```

If the tunnel port receives the frames of client VLANs 2–30 (C-Tag), the frames will be encapsulated with the tag (S-Tag) of SP VLAN 10.

```
PE(config-if-GigabitEthernet 0/1)# dot1q outer-vid 10 register inner-vid 2-30
```

If the tunnel port receives the frames of client VLANs 102–130 (C-Tag), the frames will be encapsulated with the tag (S-tag) of SP VLAN 20.

```
PE(config-if-GigabitEthernet 0/1)# dot1q outer-vid 20 register inner-vid 102-130
```

(2) On the tunnel port, replicate the priority of inner tag in the client packet to the outer tag.

```
PE(config-if-GigabitEthernet 0/1)# mls qos trust cos
PE(config-if-GigabitEthernet 0/1)# inner-priority-trust enable
PE(config-if-GigabitEthernet 0/1)# exit
```

(3) Configure the interface on the PE for connecting to the public network as an uplink port.

```
PE(config)# interface gigabitethernet 0/2
PE(config-if-GigabitEthernet 0/2)# switchport mode uplink
PE(config-if-GigabitEthernet 0/2)# end
PE# write
```

(4) Create a client VLAN on CE, and configure the interface for connecting PE as an uplink port.

```
CE> enable
CE# configure terminal
CE(config)# vlan range 2-30,102-130
CE(config-vlan)# exit
CE(config)# interface gigabitethernet 0/1
CE(config-if-GigabitEthernet 0/1)# switchport
CE(config-if-GigabitEthernet 0/1)# switchport mode uplink
CE(config-if-GigabitEthernet 0/1)# exit
```

(5) Configure the interface on the CE for connecting to the HGW as a trunk port. Gigabit Ethernet 0/2 and Gigabit Ethernet 0/30 are taken as examples below. The configurations of the other interface are similar.

```
CE(config)# interface gigabitethernet 0/2
CE(config-if-GigabitEthernet 0/2)# switchport
CE(config-if-GigabitEthernet 0/2)# switchport mode trunk
CE(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan only 2,102
CE(config-if-GigabitEthernet 0/2)# exit
CE(config)# interface gigabitethernet 0/30
CE(config-if-GigabitEthernet 0/30)# switchport
CE(config-if-GigabitEthernet 0/30)# switchport mode trunk
CE(config-if-GigabitEthernet 0/30)# switchport trunk allowed vlan only 30,130
CE(config-if-GigabitEthernet 0/30)# end
CE# write
```

5. Verification

(1) Display the PE configuration.

Display the interface configuration of the PE.

```
PE# show interfaces switchport
Interface                    Switchport Mode     Access Native Protected VLAN
lists
------------------------------- ---------- --------- ------ ------ ---------
----------------
GigabitEthernet 0/1            enabled   TUNNEL   1     1     Disabled
1,10,20
GigabitEthernet 0/2            enabled   UPLINK   1     1     Disabled  ALL
```

Display the tunnel port configuration of the PE. The outer tag VLAN has been added to the allowed VLAN list of the interface.

```
PE# show interfaces dot1q-tunnel
========Interface Gi0/1========
Native vlan: 1
Allowed vlan list:1,10,20
Tagged vlan list:
```

Verify that the encapsulation policy relationship for adding S-tags based on C-tags is correct.

```
PE# show registration-table
Ports    Type          Outer-VID   Inner-VID-list
------   ----------     ----------  --------------
Gi0/1    Add-outer      10          2-30
Gi0/1    Add-outer      20          102-130
```

Display the priority replication relationship of the interface.

```
PE# show inner-priority-trust interfaces gigabitethernet 0/1
Port   Inner-priority-trust
-----  -------------------
Gi0/1  Enable
```

(2) Display the CE configuration.

Display the interface configuration of the CE.

```
CE# show interfaces switchport
Interface                    Switchport Mode     Access Native Protected VLAN
lists
------------------------------- ---------- --------- ------ ------ ---------
----------------
GigabitEthernet 0/1            enabled   Uplink   1     1     Disabled  ALL
GigabitEthernet 0/2            enabled   Trunk    1     1     Disabled  2,102
GigabitEthernet 0/3            enabled   Trunk    1     1     Disabled  3,103
……
GigabitEthernet 0/30           enabled   Trunk    1     1     Disabled  30,130
```

6. Configuration Files

- Configuration file of the PE

```
vlan range 1,10,20
!
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 10,20
 dot1q outer-vid 100 register inner-vid 2-30
 dot1q outer-vid 200 register inner-vid 102-130
 mls qos trust cos
 inner-priority-trust enable
!
interface GigabitEthernet 0/2
 switchport mode uplink
```

- Configuration file of the CE (Only Gigabit Ethernet 0/2 and Gigabit Ethernet 0/30 are taken as examples of interfaces connected to the HGW. The configurations of the other interfaces are similar.)

```
vlan range 1-30,102-130
!
interface GigabitEthernet 0/1
 switchport mode uplink
!
interface GigabitEthernet 0/2
 switchport mode trunk
 switchport trunk allowed vlan only 2,102
!
interface GigabitEthernet 0/30
 switchport mode trunk
 switchport trunk allowed vlan only 30,130
```

1.10.3 Configuring ACL-Based Selective QinQ to Implementing Layer-2 VPN and Service Flow Management

1. Requirements

If the service flows of client network are not classified according to VLAN, but according to the MAC address, IP address, or protocol type, or there are a large number of old low-end network access devices on the client network and the service flows cannot be effectively distinguished using VLAN ID, the packets from the client network cannot be encapsulated with outer tags based on their C-tags to realize transparent transmission and implement QoS policies.

ACL can classify service flows according to the MAC address, IP address, or protocol type, and selective QinQ can distinguish different service flows using ACL, add and modify outer tags, and assign different service data to different VLANs and implement the VPN channel for transparent transmission of client services. If the SP network provides different QoS service policies for different services, it can guarantee first transmission of high-priority services.

As shown in Figure 1-6, internal networks of the company's branches in two cities are connected to CE 1 and CE 2, and then connected to the SP network through PE 1 and PE 2.

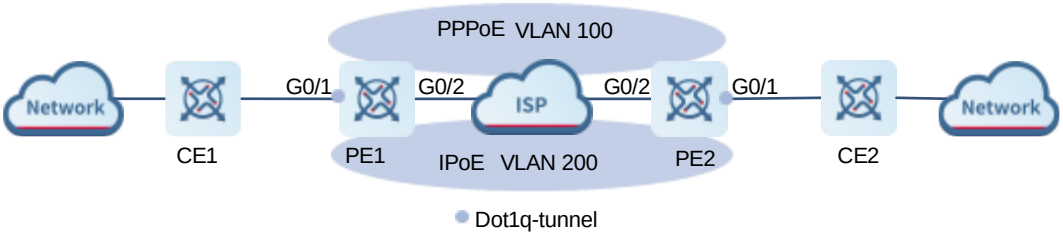
The selective QinQ function based on ACL is used on PE 1 and PE 2 to encapsulate different service data of the company with different outer VLAN tags so that the data can be transmitted through the SP network transparently and the branches can access each other's network.

- ACL 1 identifies service flows of PPPoE type and allocates the service flows to VLAN 100 for transmission.
- ACL 2 identifies service flows of IPTV (IPoE) type and allocates the service flows to VLAN 200 for transmission.

The SP network sets the QoS policy based on CoS. You can modify the CoS values of packets through priority mapping on PE 1 and PE 2 to ensure preferential transmission of service flows of the client network using the QoS policy of the SP network.

2. Topology

Figure 1-6 Selective QinQ Implements Layer-2 VPN



3. Notes

- Configure the ACL policy on PE 1 and PE 2 to distinguish different service flows of the client network: the protocol type of PPPoE packets is 0x8863 or 0x8864, and that of IPoE packets is 0x0800. Configure the interface for connecting to the CE as tunnel port, and configure the selective QinQ function based on ACL. The configuration of PE 2 is similar to that of PE 1. Only PE 1 is taken as an example in the configuration procedure.
- The SP network provides a CoS-based QoS priority policy, and the packets of client network are attached with tags. You can configure priority mapping to modify the CoS value of the outer tag. In this way, the packet is transmitted based on the corresponding QoS priority policy of the SP after being encapsulated with an outer tag, and flexible control is implemented on the packet priority on the tunnel port.

4. Procedure

(1) On the PE, create an ACL for distinguishing service flows.

```
PE1> enable
PE1# configure terminal
PE1(config)# expert access-list extended acl1
PE1(config-exp-nacl)# permit 0x8863 any any
PE1(config-exp-nacl)# permit 0x8864 any any
PE1(config-exp-nacl)# exit
PE1(config)# expert access-list extended acl2
PE1(config-exp-nacl)# permit 0x0800 any any
```

```
PE1(config-exp-nacl)# exit
```

(2) Configure the ACL-based QinQ encapsulation rule.

Add the SP VLAN 100 and VLAN 200 to the untagged VLAN list of the tunnel port GigabitEthernet 0/1.

```
PE1(config)# vlan rang 100,200
PE1(config-vlan-range)# exit
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
PE1(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan add
untagged 100,200
```

(3) Configure the outer tag priority of packets according to the inner tag priority of packets.

```
PE1(config-if-GigabitEthernet 0/1)# mls qos trust cos
PE1(config-if-GigabitEthernet 0/1)# no inner-priority-trust enable
PE1(config-if-GigabitEthernet 0/1)# dot1q-tunnel cos 3 remark-cos 5
PE1(config-if)# exit
```

(4) Configure the interface connected to the public network as an uplink port.

```
PE1(config)# interface gigabitethernet 0/2
PE1(config-if-GigabitEthernet 0/2)# switchport mode uplink
PE1(config-if-GigabitEthernet 0/2)# end
PE1# write
```

5. Verification

(1) Display the interface configuration of the PE.

```
PE1# show interfaces switchport
Interface                    Switchport Mode     Access Native Protected VLAN
lists
-------------------------------- ---------- --------- ------ ------ ---------
----------------
GigabitEthernet 0/1            enabled   TUNNEL   1     1     Disabled
1,100,200
GigabitEthernet 0/2            enabled   UPLINK   1     1     Disabled  ALL
```

(2) Display the priority mapping relationship on the interface.

```
PE1# show interfaces gigabitethernet 0/1 remark
Ports       From COS  To COS
------------ --------- --------
Gi0/1       3       5
```

(3) The clients of the same service in the company's branch can realize layer-2 VPN interworking. Specific service data can enjoy a higher transmission priority.

6. Configuration Files

Configuration files of PE 1 and PE 2

```
expert access-list extended acl1
 10 permit 0x8863 any any
 20 permit 0x8864 any any
```

```
!
expert access-list extended acl2
 10 permit 0x800 any any
!
vlan range 1,100,200
!
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 100,200
 dot1q-Tunnel cos 3 remark-cos 5
 mls qos trust cos
!
 interface GigabitEthernet 0/2
 switchport mode uplink
```

7. Common Errors

- The ACL policy is configured incorrectly. The ACL policy number is not in the parameter range. The ACL name is already taken.
- Priority replication is not disabled before priority mapping is configured.

1.10.4 Configuring Layer-2 Protocol Tunneling Based on QinQ

1. Requirements

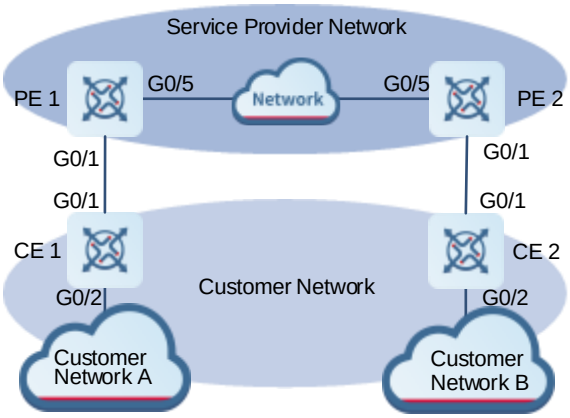
As shown in Figure 1-7, the upper part of the typical topology of QinQ network is the SP network, and the lower part is the client network. The SP network consists of PE 1 and PE 2. Customer Network A and Customer Network B are a user's two sites in different regions. CE 1 and CE 2 are access devices from the client network to the SP network, and access the SP network through PE 1 and PE 2 respectively.

The layer-2 protocol tunneling is configured to transparently transmit layer-2 protocol packets from one end to the other end of the client network so that the layer-2 protocols of the client network and the SP network are calculated separately without interference.

- Configure the STP protocol tunneling function based on user requirements to realize tunnel transmission of BPDU packets of the client network in the SP network and to perform unified spanning tree calculation for the cross-regional client network across the SP network.
- Configure the GVRP protocol tunneling function based on user requirements to realize tunnel transmission of GVRP packets of the client network and perform dynamic VLAN configuration of the client network across the SP network.

2. Topology

Figure 1-7 QinQ Implements Layer-2 Protocol Tunneling



3. Notes

- On PE 1 and PE 2, configure the STP and GVRP tunneling functions globally.
- Configure the QinQ encapsulation mode. Basic QinQ is taken as an example (for details, see "1.10.1 Configuring Basic QinQ to Implement Layer-2 VPN") to configure the native VLAN of tunnel port as VLAN 10, and VLAN 10 is used as the public network transmission channel. A client data packet is first encapsulated with one VLAN 10 tag, and then forwarded on the public network.
- Enable the STP and GVRP tunneling functions on the interface GigabitEthernet 0/1.
- Configure the uplink port.

4. Procedure

Both PE 1 and PE 2 need to be configured. The configuration method on the two devices is the same. PE 1 is taken as an example below.

(1) Enable the STP and GVRP tunneling functions globally.

```
PE1> enable
PE1# configure terminal
PE1(config)# l2protocol-tunnel stp
PE1(config)# l2protocol-tunnel gvrp
```

(2) Configure the basic QinQ transmission channel VLAN 10. VLAN 10 is the native VLAN of the tunnel port, and belongs to the allowed untagged VLAN list of the tunnel port.

```
PE1(config)# vlan 10
PE1(config-vlan)# exit
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-GigabitEthernet 0/1)# switchport
PE1(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
PE1(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel native vlan 10
PE1(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan add
untagged 10
```

(3) Enable the STP and GVRP tunneling functions on the tunnel port.

```
PE1(config-if-GigabitEthernet 0/1)# l2protocol-tunnel stp enable
PE1(config-if-GigabitEthernet 0/1)# l2protocol-tunnel gvrp enable
PE1(config-if-GigabitEthernet 0/1)# exit
```

(4) Configure the uplink port.

```
PE1(config)# interface gigabitethernet 0/5
PE1(config-if-GigabitEthernet 0/5)# switchport
PE1(config-if-GigabitEthernet 0/5)# switchport mode uplink
PE1(config-if-GigabitEthernet 0/5)# end
PE1# write
```

5. Verification

The verification method is the same on PE1 and PE2. PE 1 is taken as an example below.

Verify that the STP tunneling function is enabled globally and on the interface at the same time.

```
PE1# show l2protocol-tunnel stp
L2protocol-tunnel: Stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
GigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Verify that the GVRP tunneling function is enabled globally and on the interface at the same time.

```
PE1# show l2protocol-tunnel gvrp
L2protocol-tunnel: Gvrp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0006
GigabitEthernet 0/1 l2protocol-tunnel gvrp enable
```

6. Configuration Files

Configuration files of PE 1 and PE 2

```
l2protocol-tunnel stp
l2protocol-tunnel gvrp
!
vlan range 1,10
!
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 10
 switchport dot1q-tunnel native vlan 10
 l2protocol-tunnel stp enable
 l2protocol-tunnel gvrp enable
!
interface GigabitEthernet 0/5
 switchport mode uplink
```

7. Common Errors

- The layer-2 tunneling function is not enabled globally and on the interface at the same time, and therefore it fails to take effect.
- In the SP network, the configured BPDU tunnel addresses are inconsistent, and therefore BPDU frames of the client network cannot be correctly transmitted.

Contents

1 Configuring MSTP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Background and Functions 1
1.1.3 STP 2
1.1.4 RSTP 12
1.1.5 MSTP 18
1.1.6 Protocols and Standards 27
1.2 Configuration Task Summary 27
1.2.1 Configuring STP 27
1.2.2 Configuring RSTP 27
1.2.3 Configuring MSTP 28
1.2.4 Configuring Advanced Functions for Spanning Trees 28
1.2.5 Configuring BPDU Transparent Transmission 29
1.3 Configuring the Spanning Tree Mode 29
1.3.1 Overview 29
1.3.2 Restrictions and Guidelines 29
1.3.3 Procedure 29
1.4 Configuring an MST Region 30
1.4.1 Overview 30
1.4.2 Restrictions and Guidelines 30
1.4.3 Prerequisites 30

1.4.4 Procedure.....30

1.5 Configuring the Bridge Priority and Port Priority.....31

1.5.1 Overview.....31

1.5.2 Restrictions and Guidelines.....31

1.5.3 Procedure.....31

1.6 Configuring the Port Path Cost.....32

1.6.1 Overview.....32

1.6.2 Restrictions and Guidelines.....32

1.6.3 Configuration Tasks.....32

1.6.4 Configuring the Path Cost Calculation Method.....33

1.6.5 Configuring the Path Cost Value.....34

1.7 Configuring Spanning Tree Time Parameters.....35

1.7.1 Overview.....35

1.7.2 Restrictions and Guidelines.....35

1.7.3 Procedure.....36

1.8 Configuring the Maximum Hop Count for BPDUs.....36

1.8.1 Overview.....36

1.8.2 Restrictions and Guidelines.....36

1.8.3 Procedure.....37

1.9 Configuring Fast Convergence of Spanning Trees.....37

1.9.1 Overview.....37

1.9.2 Restrictions and Guidelines.....37

1.9.3 Procedure.....37

1.10 Enabling Protocol Migration.....38

1.10.1 Overview 38

1.10.2 Procedure 38

1.11 Configuring Spanning Tree Compatibility for Interfaces 39

1.11.1 Overview 39

1.11.2 Procedure 39

1.12 Enabling the STP Function 39

1.12.1 Overview 39

1.12.2 Restrictions and Guidelines 39

1.12.3 Procedure 39

1.13 Configuring Port Protection 40

1.13.1 Overview 40

1.13.2 Restrictions and Guidelines 40

1.13.3 Configuration Tasks 40

1.13.4 Configuring Root Guard 40

1.13.5 Configuring Loop Guard 41

1.14 Configuring BPDU Source MAC Address Check 42

1.14.1 Overview 42

1.14.2 Restrictions and Guidelines 42

1.14.3 Prerequisites 43

1.14.4 Procedure 43

1.15 Configuring an Edge Port 43

1.15.1 Overview 43

1.15.2 Restrictions and Guidelines 43

1.15.3 Configuration Tasks 44

1.15.4 Configuring Autoedge 44

1.15.5 Configuring the Port Fast Attribute 44

1.16 Configuring BPDU Guard or BPDU Filter 46

1.16.1 Overview 46

1.16.2 Restrictions and Guidelines 46

1.16.3 Configuration Tasks 46

1.16.4 Configuring BPDU Guard 46

1.16.5 Configuring BPDU Filter 47

1.17 Configuring TC Attack Defense Functions 48

1.17.1 Overview 48

1.17.2 Restrictions and Guidelines 49

1.17.3 Configuration Tasks 49

1.17.4 Configuring TC Protection 49

1.17.5 Configuring TC Guard 50

1.17.6 Configuring TC Filter 50

1.18 Configuring BPDU Tunnel 51

1.18.1 Overview 51

1.18.2 Restrictions and Guidelines 52

1.18.3 Procedure 52

1.19 Configuring BPDU Transparent Transmission 52

1.19.1 Overview 52

1.19.2 Restrictions and Guidelines 53

1.19.3 Procedure 53

1.20 Monitoring 53

1.21 Configuration Examples.....55

1.21.1 Configuring MSTP.....55

1.21.2 Configuring MSTP+VRRP 70

1.21.3 Configuring Spanning Tree Compatibility for MSTP Interfaces.....83

1.21.4 Configuring BPDU Tunnel.....89

1.21.5 Configuring BPDU Transparent Transmission.....97

1 Configuring MSTP

1.1 Introduction

1.1.1 Overview

The Spanning Tree Protocol (STP) is an L2 management protocol used to eliminate L2 loops by blocking redundant links in the network. It enables a backup link in the case of a link failure.

With the network development and update, multiple STP versions become available. This device supports STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP).

1.1.2 Background and Functions

1. 802.1D STP

To prevent single point of failures (SPOFs), L2 devices enhance line reliability by adding redundant lines. One of the most economical ways is to add loops. However, loops may cause broadcast storms and Media Access Control (MAC) address flapping. Therefore, the STP protocol arises.

STP can generate the best loop-free tree topology for a local area network (LAN) via computation. If detecting a fault, STP automatically eliminates the fault and updates the topology.

STP cannot enter forwarding state quickly but needs 50 seconds to complete topology convergence. All virtual local area networks (VLANs) in an LAN share one spanning tree. Packets of all the VLANs are forwarded along this spanning tree, and the bandwidth of redundant lines is wasted. VLAN data may be isolated at L2, and L2 loops do not exist in some circumstances. However, STP cannot recognize VLANs, and packets from interfaces in the same VLAN may be intercepted by blocking ports, resulting in a communication failure.

2. 802.1w RSTP

RSTP is fully compatible with STP backward. Apart from the conventional STP functions of eliminating loops and enabling backup links, RSTP solves the problem of entering forwarding state rapidly. If all bridges in a LAN support RSTP and are properly configured, once the network topology changes, RSTP takes only less than 1s to regenerate a topology tree.

Although RSTP can complete convergence quickly, it cannot identify VLANs just as STP does not.

3. 802.1s MSTP

MSTP resolves defects of STP and RSTP. It not only supports fast convergence but also forwards traffic of different VLANs along their respective paths, thereby providing a better load balancing mechanism for redundant links. STP/RSTP works based on ports while MSTP works based on instances. An instance is a collection of multiple VLANs. Binding multiple VLANs to one instance can reduce communication costs and improve resource usage. MSTP can implement the following functions:

- When lines are normal, MSTP can eliminate loops and prevent broadcast storms and MAC address flapping, to ensure normal L2 communication.
- When a line is faulty, MSTP enables a backup link to enhance the link reliability. It can complete convergence rapidly to enhance the link availability.

- MSTP can produce multiple spanning trees by VLAN instance to implement traffic balancing.

1.1.3 STP

1. Overview

STP, defined by the Institute of Electrical and Electronics Engineers (IEEE) 802.1D standard, is used to break physical loops at the data link layer in a LAN and prevent broadcast storms, so as to implement link redundancy.

L2 devices connected using single lines have no redundant lines and devices. Any SPOF can cause device disconnection and the line reliability is low. When a redundant line is added, an L2 loop will form and the SPOF can be eliminated.

The adding of a redundant line brings two new problems:

- Once a broadcast frame appears in an L2 loop, it will be flooded continuously by L2 devices and a broadcast storm will be incurred, which will heavily consume device resources and network bandwidth.
- In a loop topology, an L2 device may receive packets from the same source MAC address through two ports of two paths, causing MAC address flapping and the failure of the device to work properly.

Therefore, for L2 Ethernet, only one valid channel is required to forward data between two LANs. Ideally, when an L2 loop exists on a network, a specific port can be blocked to invalidate the redundant link so as to break the loop; when a network fault occurs, the specific port can be enabled to restore a redundant link to the valid state. It is difficult to attain this ideal effect via manual control. Therefore, the STP protocol emerges to automatically complete this work:

- Devices with STP enabled exchange specific STP Protocol Packets, that is, bridge protocol data units (BPDUs), and elect Device Roles (root bridge and non-root bridge) and Port Roles (root port, designated port, and blocking port) based on Key Information of BPDUs. Different port roles are in different Port States and have different functions. They form a Generating a Spanning Tree Topology in a LAN.
- Protocol packets are used to monitor the line status to Maintaining a Spanning Tree Topology. Once a fault is found, STP rectifies the fault and automatically Updating a Spanning Tree Topology.

2. STP Protocol Packets

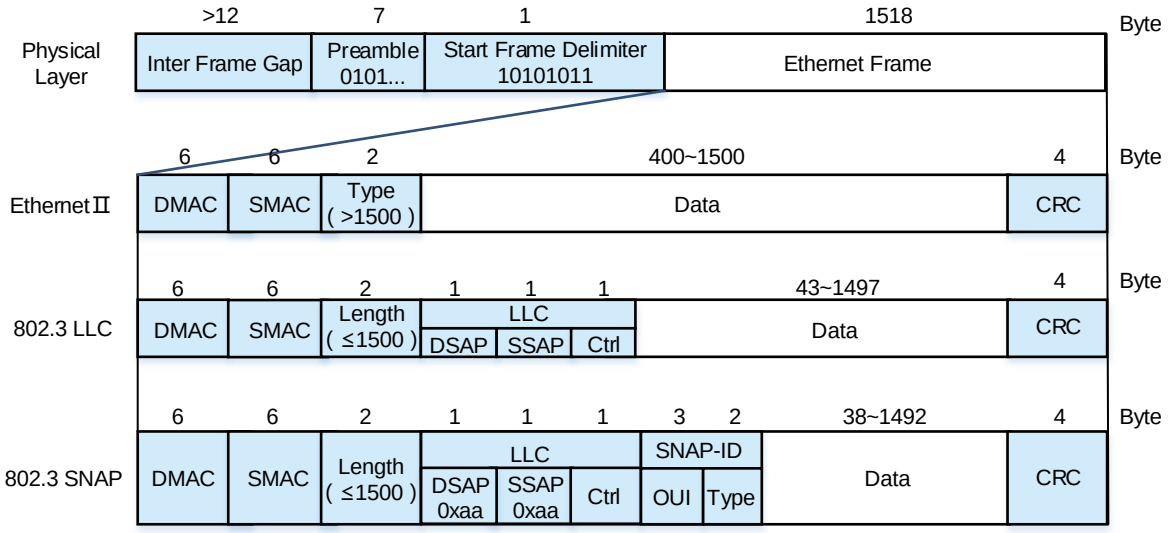
STP uses two types of protocol packets: configuration BPDU and topology change notification (TCN) BPDU.

- Configuration BPDU: A configuration BPDU contains 35 bytes, which provide information required for calculating the spanning tree topology (root bridge ID, root path cost, designated bridge ID, and designated port ID) and information required for maintaining the spanning tree (**Message Age**, **Max Age**, **Hello Time**, and **Forward Delay**). When STP is enabled on a designated port, the port sends configuration BPDUs at an interval of **Hello Time**. When a device receives a configuration BPDU from a root port, it sends the configuration BPDU to each designated port on the device, and the designated ports generate their own BPDUs. If the configuration BPDU received by a designated port from the line has a lower priority than the BPDU generated by the designated port itself (see Key Information of BPDUs), the designated port sends its BPDU to the downstream device.
- TCN BPDU: A TCN BPDU contains four bytes. On a bridge with at least one designated port, when a port on the bridge transitions to forwarding or blocking state, the network topology has changed. The bridge will send a TCN BPDU to inform the upstream device of the network topology change. When the upstream device receives the TCN BPDU through a designated port, it sets TCA in the configuration BPDU to 1 and instructs the downstream device to stop sending the TCN BPDU. The upstream device also sends a copy of

the TCN BPDU to its upstream device until the TCN BPDU reaches the root bridge. By setting the TC flag bit in the configuration BPDU to 1, the root bridge informs all bridges in the spanning tree of the network topology change, and asks them to clear dynamic MAC address entries of ports and relearn MAC addresses. A shorter MAC address aging time facilitates fast convergence of the topology.

BPDUs are encapsulated in IEEE 802.3 logical link control (LLC) Ethernet frames. The format differences between BPDUs and other Ethernet frames are as follows.

Figure 1-1 Formats of Ethernet Frames



An actual STP configuration BPDU is taken as an example for description.

Figure 1-2 STP Configuration BPDU

```
0000  01 80 c2 00 00 00 00 d0  f8 22 35 4a 00 26 42 42
0010  03 00 00 00 00 00 80 00  00 d0 f8 22 35 4a 00 00
0020  00 00 80 00 00 d0 f8 22  35 4a 80 1c 00 00 14 00
0030  02 00 0f 00 00 00 00 00  00 00 00 00
```

The header of an IEEE 802.3 Ethernet frame contains 14 bytes and the fields in the header are described in Table 1-1.

Table 1-1 Description of Fields in the Header of an IEEE 802.3 Ethernet Frame

Field	Bytes	Description
DMAC	6	Destination MAC address. According to the protocol, the destination address of the Ethernet frame used for encapsulating a BPDU is fixed to the multicast address 0180.c200.0000. A device receiving a frame with such a destination address will not forward the frame.
SMAC	6	Source MAC address of the device sending the BPDU. The value in the example is 00-d0-f8-22-35-4a.

Field	Bytes	Description
Length	2	The value is 0x0026, indicating that the packet length is 38 bytes (3 bytes of the LLC header and 35 bytes of the BPDU).

The LLC header occupies three bytes, which are described in Table 1-2.

Table 1-2 Description of Fields in the LLC Header of an Ethernet Frame

Field	Bytes	Description
DSAP	1	Destination service access point. The value is 0x42.
SSAP	1	Source service access point. The value is 0x42.
Control	1	This field stores various control information and identifies the type of an LLC frame. The value is 0x03.

The bytes behind the LLC header is a BPDU. There are four types of BPDUs for STP, RSTP, and MSTP, which are differentiated using different PVIDs and BPDU type values.

A configuration BPDU of STP occupies 35 bytes, which are described in Table 1-3. The last part is an 8-byte filling field and a 4-byte CRC field (not shown in the figure). They form a 64-byte Ethernet frame.

Table 1-3 Format of an STP Configuration BPDU

Field	Bytes	Description
PID	2	Protocol identifier. The value is 0x0000.
PVID	1	Protocol version identifier. 0x00 indicates an STP packet.
BPDU Type	1	BPDU packet type. 0x00 indicates a configuration BPDU of STP.
Flags	1	The value is 0x00 in the example. Configuration BPDUs of STP use only bit 7 and bit 0 and other bits are not used. ● Bit 7: Topology change acknowledgment (TCA). An upstream device sets bit 7 in a configuration BPDU to 1 and sends the BPDU to notify the downstream device of the topology change and requests the downstream device to stop sending the TCN BPDU. ● Bit 0: Topology change (TC). The root bridge sets bit 0 in a configuration BPDU to 1 and sends the BPDU to instruct the downstream device to directly delete MAC address entries of the bridges.
Root ID	8	Identifier of the root bridge recognized by the device. It consists of a 2-byte bridge priority and a 6-byte bridge MAC address. In the example, the priority value is 0x8000, which indicates 32768, and the bridge MAC address is 00-d0-f8-22-35-4a.

Field	Bytes	Description
RPC	4	Root path cost, which is the cumulative cost from the port to the root bridge. The value is 0x00-00-00-00 in the example.
Bridge ID	8	Bridge identifier of the device. It consists of a 2-byte bridge priority and a 6-byte bridge MAC address. In the example, the priority value is 0x8000, which indicates 32768, and the bridge MAC address is 00-d0-f8-22-35-4a.
Port ID	2	Identifier of the port that sends the BPDU. It consists of a 1-byte priority and 1-byte port ID. In the example, the priority value is 0x80, which indicates 128, and the port ID is 1c.
Message Age	2	Age of the BPDU, which represents the time that the BPDU has been alive in the network. The value is 0x0000 in the example.
Max Age	2	Aging time of the BPDU. If a non-root bridge fails to receive a BPDU from the root bridge within the time of **Max Age**, the root bridge or the link to the root bridge is deemed as faulty. The value in the example is 0x1400 (low-order bytes on the left), indicating 20 seconds.
Hello Time	2	Interval for sending two adjacent BPDUs. The root bridge sends configuration BPDUs at an interval of **Hello Timer**. A non-root switch sends a configuration BPDU only after receiving the configuration BPDU from the upstream device. The value in the example is 0x0200 (low-order bytes on the left), indicating 2 seconds.
FWD Delay	2	Forwarding delay. This time parameter controls the duration of listening and learning states. The value in the example is 0x0f00 (low-order bytes on the left), indicating 15 seconds.

A TCN BPDU consists of four bytes and contains only the **PID**, **PVID**, and **BPDU Type** fields. The packet format is described in Table 1-4.

Table 1-4 Format of an STP TCN BPDU

Field	Bytes	Description
PID	2	Protocol identifier. The value is 0x0000.
PVID	1	Protocol version identifier. 0x00 indicates an STP packet.
BPDU Type	1	BPDU packet type. 0x80 indicates a TCN BPDU of STP. When the downstream network topology changes, it is used to notify the upstream device of the network topology change. After receiving a TCN BPDU, a port copies the BPDU and forwards it to upstream devices till the root device receives the BPDU.

3. Key Information of BPDUs

- Priority vector

  Bridges exchange BPDUs to obtain information and generate a stable optimal tree topology. The most basic elements in the information are listed as follows:

  - Root ID: ID of the root bridge recognized by this local bridge. It consists of the bridge priority and MAC address of the root. The root bridge ID is the bridge ID of the root.
  - Root Path Cost: Path cost from this bridge to the root bridge.
  - Bridge ID: Each bridge has a unique bridge ID consisting of the bridge priority and MAC address.
  - Port ID: ID of each port, which consists of the port priority and port ID.

  These key elements constitute a priority vector <**Root Identifier**, **Root Path Cost**, **Bridge ID**, **Port ID**>. Bridges compare elements in the priority vector in sequence to determine the priority of BPDUs. A smaller priority element value indicates a higher priority. If a port of a bridge receives a BPDU with the priority higher than the BPDU priority of the port, the port saves and transmits the BPDU. If it receives a BPDU with the priority lower than the BPDU priority of the port, in case of STP, it discards the BPDU, but in case of RSTP or MSTP, it will send a Proposal BPDU to request the peer to recognize the local device as the upstream device. This mechanism ensures that high-priority BPDUs are transmitted throughout the network.

- Bridge ID

  According to IEEE 802.1W, a root ID is used to identify a root bridge in a spanning tree while a bridge ID is used to identify each bridge. When a device just runs STP, it uses its bridge ID as the root ID and STP compares root IDs to elect the root bridge according to algorithms. A bridge ID consists of eight bytes, with the first two bytes of the bridge priority and the last six bytes of the bridge MAC address. A device compares the bridge priority first and then the MAC address during root bridge selection. A smaller value indicates a higher priority.

  Bridge priority: To ensure network reliability, you are advised to specify bridge priorities during network planning, to prevent devices from electing the root bridge by comparing MAC addresses. In the 2-byte bridge priority, bit 1 to bit 12 indicate the system ID used for protocol extension and the value is **0** in RSTP. Bit 13 to bit 16 indicate the priority, which can be configured. If the configured priority is 0001 0000 0000 0000 (**4096** in decimal notation), the bridge priority is a multiple of 4096. Bit 13 to bit 16 can indicate 15 numbers from 0000 to 1111. Therefore, the priority is 4096 × 0 to 4096 × 15 in decimal notation.

Table 1-5 Bridge Priority Field (Two Bytes)

	Priority				**System ID**											
Bit	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
Value	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

- Port ID

  Each port participating in the spanning tree calculation must have a port ID, which is the port ID of a device.

  Format: A port ID consists of two bytes, with the first byte of the port priority and the second byte of the port ID.

The default port priority is **128** and the port priority range is from 0 to 255. The port ID range is from 0 to 255, for example, the ID (0) of port GigabitEthernet 0/0 is smaller than that (1) of port GigabitEthernet 0/1.

- Root path cost

  Root path cost is the cumulative path cost from the port to the root bridge. A link between two directly connected ports is called a "segment". A segment with a higher network bandwidth has a lower path cost. The total cost calculated based on the path costs of all ports in the necessary lines from a port to the root is the cumulative path cost from the port to the root bridge. Table 1-6 shows the cost values supported by different protocols. Path cost values defined for the device are provided in Table 1-11.

Table 1-6 Path Costs Supported by Protocols

Bandwidth	RPC Supported by IEEE 802.1t	RPC Supported by IEEE 802.1d
10 Mbps	2000000	100
100 Mbps	200000	19
1 Gbps	20000	4
10 Gbps	2000	2

4. Device Roles

Devices with STP enabled exchange BPDUs and compare root IDs to elect device roles.

- Root bridge: Each spanning tree has a unique root.
- Designated bridge: A device in the shortest path between the local device and the root bridge, that is, the upstream device of the local device.
- Bridge: Generally the local device, that is, downstream device of a designated bridge. Designated bridges and bridges can be collectively referred to as non-root bridges.

5. Port Roles

The root bridge and non-root bridges elect different port roles by exchanging BPDUs.

- Root port: A port with the shortest path from a non-root bridge to the root bridge.
- Designated port: Each port on the root bridge is a designated port. The root bridge connects to a root port of a non-root bridge through a designated port. The port that connects a designated bridge to a downstream device is also a designated port.
- Disable port: Also called a blocking port. A disable port is a port in blocked or down state on a non-root bridge.

6. Port States

Ports work in different states and perform different functions according to the protocol. Table 1-7 lists functions corresponding to port states.

STP defines five port states: disabled, blocking, listening, learning, and forwarding. RSTP reduces port states to only three states: discarding, learning, and forwarding. MSTP uses the port states of RSTP.

Table 1-7 Port Roles, Port States, and Functions Supported by STP, RSTP, and MSTP

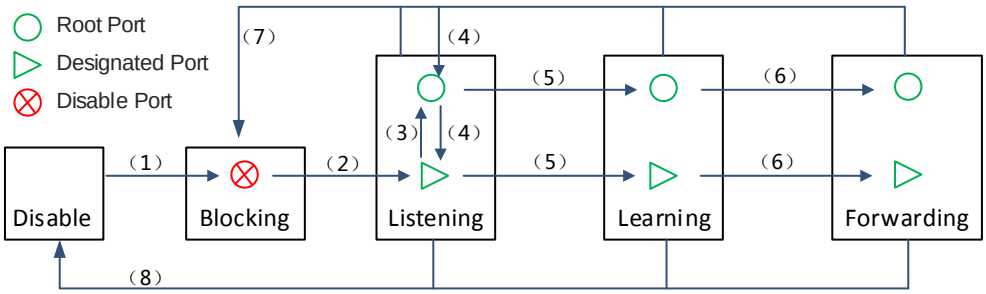
Note: In this table, R = root port, D = designated port, A = alternate port, B = backup port, BLK = blocking port.

STP		RSTP and MSTP		Function				
Port Role	**Port State**	**Port Role**	**Port State**	**Receiving BPDUs**	**Sending BPDUs**	**MAC Address Learning**	**Receiving Data**	**Forwarding Data**
Disable	Disabled	Disable	Discarding	No	No	No	No	No
Blk	Blocking	A, B	Discarding	Blk, A, B	No	No	No	No
R, D	Listening	R, D	Discarding	R, D	D	No	No	No
	Learning		Learning	R, D	D	R, D	No	No
	Forwarding		Forwarding	R, D	D	R, D	R, D	R, D

After a topology becomes stable, only root ports and designated ports are in forwarding state and can send and receive data. Other ports are in blocking state and can only receive BPDUs. Different port roles have different functions in the same port state. For example, a root port cannot send but can receive BPDUs in forwarding state, while a designated port can send and receive BPDUs in forwarding state.

The port states can be transitioned according to the rules shown in Figure 1-3.

Figure 1-3 State Transition Rules of STP Ports



(1) After being initialized or enabled, a port enters blocking state.

(2) When STP is just running on a device, all the ports on the device enter listening state as designated ports, and send and receive BPDUs for election. After STP runs stably, if a blocking port fails to receive a BPDU within **MAX Age**, it becomes a designated port, transitions from blocking state to listening state, and receives and sends BPDUs for re-election.

(3) After election, if a port is elected as a root port, it only receives BPDUs but cannot send BPDUs.

(4) If a root port fails to receive a BPDU within **MAX Age**, the root is considered to be faulty, and the root port becomes a designated port and sends a BPDU.

(5) After a port is elected as a root port or designated port, it waits for one period of **Forward Delay**, transitions from listening state to learning state, and starts MAC address learning.

(6) Then, the port waits for another period of **Forward Delay**, transitions from learning state to forwarding state, and starts sending and receiving BPDUs.

(7) If the port is no longer a root port or designated port, it returns to blocking state.

(8) If a port is disabled or the link is faulty, the port returns to disable state.

7. Generating a Spanning Tree Topology

STP automatically calculates and generates a spanning tree topology for a LAN according to a set of bridge parameters configured by the administrator. Only appropriate configuration can ensure the fast generation of a stable topology. The steps for STP to generate a spanning tree topology are as follows:

(1) When a network starts to run STP, all switches consider themselves as root bridges and all ports on the switches are considered as designated ports. So, all ports enter listening state, broadcast configuration BPDUs, and receive BPDUs from the network. At this time, the root ID in the BPDU of each switch is the bridge ID of the switch.

(2) Each broadcast domain selects one root bridge. Each switch receives BPDUs from other switches and each BPDU contains the priority vector <**Root ID**, **Root Path Cost**, **Bridge ID**, **Port ID**>. According to the rule that a smaller value indicates a higher priority, each switch compares root IDs (bridge ID of each switch at first) in BPDUs. When a port of a switch receives a smaller root ID, the root ID is updated in the **Root ID** field in the configuration BPDUs stored in all ports of the switch and then sent to other switches. After interaction, the bridge ID of the device with the highest priority is recorded as the root ID, indicating that the device is elected as the root bridge.

(3) All ports on the root bridge are designated ports. After waiting for one period of **Forward Delay**, designated ports transition from listening state to learning state to learn MAC addresses. After waiting for another period of **Forward Delay**, the designated ports transition from learning state to forwarding state and start receiving and sending packets.

(4) Each non-root bridge compares the cumulative path cost from each port to the root and elects the port with the smallest cost as the root port. Root ports only receive configuration BPDUs from designated ports and do not send configuration BPDUs. After waiting for one period of **Forward Delay**, root ports transition from listening state to learning state to learn MAC addresses. After waiting for another period of **Forward Delay**, root ports transition from learning state to forwarding state and start sending and receiving packets.

(5) A link between two directly connected switches is called a "segment". The priority vector <**Root ID**, **Root Path Cost**, **Bridge ID**, **Port ID**> is compared in sequence to select a designated port for each segment. After waiting for one period of **Forward Delay**, designated ports transition from listening state to learning state to learn MAC addresses. After waiting for another period of **Forward Delay**, the designated ports transition from learning state to forwarding state and start receiving and sending packets.

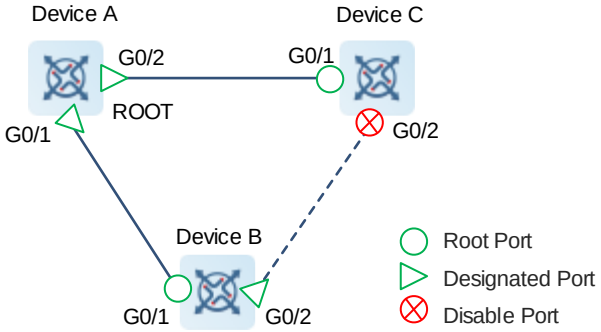
(6) The other ports are non-designated ports and are blocked. Such ports return to blocking state and only receive BPDUs. If a blocking port receives a high-priority BPDU within **MAX Age**, the current line from the peer device to the root is better and the blocking port remains in blocking state. If a blocking port fails to receive a high-priority BPDU within **MAX Age**, the current line from the peer device to the root is worse or even faulty. The blocking port transitions to listening state and sends its configuration BPDU to inform the peer device that the communication line passing through this port is better.

Note

- In STP and RSTP, the same device has the same bridge ID and the same port has the same port ID.

- In MSTP, different bridge IDs can be configured for the same device and different port IDs can be configured for the same port by instance.

Figure 1-4 Basic Topology of STP



8. Maintaining a Spanning Tree Topology

After a spanning tree topology becomes stable, only designated ports and root ports are in forwarding state while other ports are in blocking state. The root bridge continues to send configuration BPDUs at an interval of **Hello Time**. A downstream non-root bridge stores the optimal configuration BPDU received from the root port in the device, fills the bridge ID of the root bridge in the root ID, and then sends the configuration BPDU to the downstream device through a designated port. If a downstream device receives a higher-priority BPDU from the upstream device within one period of **Max Age**, the network topology remains unchanged.

9. Updating a Spanning Tree Topology

Taking the topology shown in Figure 1-4 as an example, this section describes the update process of the spanning tree topology. To simplify the description, the priority vector is <RID, Cost, BID, PID >, BIDs of Device A, Device B, and Device C are 1, 2, and 3 respectively. PIDs of ports GigabitEthernet 0/1 and GigabitEthernet 0/2 are 1 and 2 respectively. The lines are 1000M links and the path cost of each segment of line is 4.

- Device B and Device C consider themselves as root devices if the following situation occurs: Root bridge A malfunctions, Device B fails to receive BPDU<1,0,1,1> from the root bridge, and Device C fails to receive BPDU<1,0,1,2> from the root bridge within one period of **Max Age**. Then, port GigabitEthernet 0/2 of Device B sends BPDU<2,0,2,2>. Port GigabitEthernet 0/2 of Device C becomes a designated port and sends BPDU<3,0,3,2>. <2,0,2,2> has a higher priority than <3,0,3,2>. Therefore, Device B is elected as the root bridge and port GigabitEthernet 0/2 of Device C becomes a root port.
- Device C deems that root bridge A is faulty and considers itself as the root bridge if the following situation occurs: Port GigabitEthernet 0/2 of root bridge A or the link from root bridge A to Device C is faulty and downstream Device C fails to receive BPDU<1,0,1,2> from root bridge A through the root port GigabitEthernet 0/1 within one period of **Max Age**. Blocking port GigabitEthernet 0/2 (that can only receive BPDUs but cannot send BPDUs) of Device C becomes a designated port, transitions from blocking state to listening port, and sends BPDU<3,0,3,2>. Port GigabitEthernet 0/2 of Device C receives BPDU<1,4,2,2> from designated port GigabitEthernet 0/2 of Device B and finds that the root ID has a higher priority than the root ID in Device C. Device C considers Device A as the root bridge again, updates the spanning tree

topology, and sets port GigabitEthernet 0/2 as the root port. After waiting for one period of **Forward Delay**, port GigabitEthernet 0/2 transitions to learning state to learn MAC addresses. After waiting for another period of **Forward Delay**, port GigabitEthernet 0/2 transitions to forwarding state to forward data, implementing link auto-recovery. In this case, the link recovery needs **Max Age** + 2 × FWD time. The default link recovery time is 50s, that is, 20 + 2 × 15 = 50.

- Device B deems that root bridge A is faulty and considers itself as the root bridge if the following situation occurs: Port GigabitEthernet 0/1 of Device A or the link from root bridge A to Device B is faulty and downstream Device B fails to receive BPDU<1,0,1,1> from root bridge A through the root port GigabitEthernet 0/1 within one period of **Max Age**. The BPDU sent by port GigabitEthernet 0/2 of Device B changes from <1,4,2,2> (Device A functions properly) to <2,0,2,2> (Device A is faulty). Blocking port GigabitEthernet 0/2 of Device C finds that the BPDU sent from port GigabitEthernet 0/2 of Device B has a lower priority than the configuration BPDU<1,4,3,2> stored by the blocking port itself, and discards the BPDU sent from Device B. If blocking port GigabitEthernet 0/2 of Device C fails to receive a BPDU with the priority higher than that of the BPDU stored in the blocking port within one period of **Max Age**, the blocking port becomes a designated port and sends its stored BPDU<1,4,3,2> to Device B. Device B find that BPDU<1,4,3,2> has a higher priority than BPDU<2,0,2,2> stored in port GigabitEthernet 0/2 of Device B, deems that Device A is the root bridge, and sets port GigabitEthernet 0/2 as the root port. After two periods of **Forward Delay** elapse, port GigabitEthernet 0/2 of Device B transitions to forwarding state to forward data, implementing link auto-recovery in the STP network.
- If a port on a downstream device changes to down state, the device sends a TCN BPDU to the upstream device to notify the upstream device of the topology change. After receiving the TCN BPDU from the downstream device, the upstream device sets bit 7 (indicating TCA) in the **Flags** field of the configuration BPDU to **1**, and sends the configuration BPDU to the downstream device, indicating that the upstream device has known the topology change and requesting the downstream device to stop sending the TCN BPDU. Only the designated port of the upstream device processes TCN BPDUs. Non-designated ports discard TCN BPDUs directly once they receive such BPDUs. The upstream device copies the TCN BPDU and forwards it to its upstream device through the root port. The TCN BPDU is forwarded segment by segment until it reaches the root bridge. After receiving the TCN BPDU from a downstream device, the root bridge sets bit 7 (indicating TCA) in the **Flags** field of the configuration BPDU to **1** and sends the configuration BPDU to the downstream device, indicating that the upstream device has known the topology change and requesting the downstream device to stop sending the TCN BPDU. In addition, the root bridge sets bit 0 (indicating a TC) in the **Flags** field of the configuration BPDU to **1** to ask all downstream devices to clear dynamic MAC address entries of ports and relearn MAC addresses due to the topology change.
- If a new Device D is connected to Device B and the port status of Device B becomes up, Device B will also notify others of the topology change. Device D will send and receive BPDUs. If Device D has a higher priority than the original root (Device A), great changes may be incurred to the spanning tree. In conclusion, STP is not stable.

10. Drawbacks of STP

- Topology convergence is slow. After port role election is complete, STP waits for twice the period of **Forward Delay** (15s by default) before entering forwarding state, namely, STP needs to wait 30 seconds (that is, 2 × 15). Every time the topology changes, a bridge needs to re-elect the root port and designated ports after the period of **MAX Age** (20s by default), and then wait for twice the period of **Forward Delay** before entering forwarding state. Therefore, it takes about 50s (that is, 20 + 2 × 15 = 50 seconds) to generate a stable

topology. STP requires the root bridge to actively send configuration BPDUs and other devices to forward the BPDUs. This mechanism leads to slow network convergence.

- If the network topology changes frequently, the network will be frequently disconnected, which is unacceptable to users.

1.1.4 RSTP

1. Overview

RSTP, defined by IEEE 802.1W, evolves from STP and is completely compatible with IEEE 802.1D STP downward. RSTP has all functions of the conventional STP protocol and is capable of preventing loops and providing redundant links. Compared with STP, RSTP shortens the time required for network topology convergence. If all the bridges in a LAN support RSTP and are configured properly, once the network topology changes, the time required by RSTP to re-generate the topology tree is less than 1s while STP needs about 50s.

2. RSTP Protocol Packets

RSTP needs only one type of protocol packet: configuration BPDU. The packet format is slightly different from that in STP. The configuration BPDU of RSTP is also called rapid spanning tree BPDU (RST BPDU).

When a topology changes, RSTP no longer uses a TCN BPDU to notify the topology change. Instead, RSTP sets the TC bit in the **Flags** field of the RST BPDU to **1** and notifies the entire network of the topology change via RST BPDU flooding.

Figure 1-5 Configuration BPDU of RSTP

```
0000  01 80 c2 00 00 00 00 d0  f8 22 35 4a 00 27 42 42
0010  03 00 00 02 02 7c 80 00  00 d0 f8 22 35 4a 00 00
0020  00 00 80 00 00 d0 f8 22  35 4a 80 1c 00 00 14 00
0030  02 00 0f 00 00 65 20 54  79 70 65 00
```

As shown in Figure 1-5, the **Length** field is 0x0027, which indicates that the BPDU length is 39 bytes, including a 3-byte LLC header and a 36-byte RST BPDU. The BPDU starts from the 18th byte. The fields are described in Table 1-8.

Table 1-8 Format of an RST BPDU

Field	Bytes	Description
PID	2	Protocol identifier. The value is **0x0000**.
PVID	1	Protocol version identifier. The value is **0x02**, indicating an RSTP packet. Devices running STP will discard RST BPDUs upon receiving.
BPDU Type	1	BPDU packet type. The value is **0x02**, indicating an RST BPDU.

Field	Bytes	Description

Flags	1	An RST BPDU uses all the eight bits. In the example, the value is 0x7c, that is, 0111 1100.
		● Bit 7: TCA. The value **1** indicates that a topology change is known.
		● Bit 6: Agreement. The value **1** indicates consent to status switching.
		● Bit 5: Forwarding. The value **1** indicates that forwarding is allowed.
		● Bit 4: Learning. The value **1** indicates that learning is allowed.
		● Bit 3 and bit 2: Port role.
		  ○ **00**: Unknown.
		  ○ **01**: Root port.
		  ○ **10**: Alternate/Backup.
		  ○ **11**: Designated port.
		● Bit 1: Proposal. The value **1** indicates sending a proposal to request status switching.
		● Bit 0: TC. The value **1** indicates notifying the topology change.

Root ID	8	Identifier of the root bridge recognized by the device. It consists of a 2-byte bridge priority and a 6-byte bridge MAC address.
RPC	4	Root path cost, which is the cumulative path cost from the port to the root bridge.
Bridge ID	8	Bridge identifier of the device. It consists of a 2-byte bridge priority and a 6-byte bridge MAC address.
Port ID	2	Identifier of the port that sends the BPDU. It consists of a 1-byte priority and 1-byte port ID.
Message Age	2	Age of the BPDU, which represents the time that the BPDU has been alive in the network.
Max Age	2	Aging time of the BPDU.
Hello Time	2	Interval for sending two adjacent BPDUs. After an RSTP topology becomes stable, a non-root switch automatically sends configuration BPDUs at an interval of **Hello Timer** regardless of whether it receives the configuration BPDU from the root bridge. If a non-root bridge fails to receive a BPDU from the root within the time of **Time-factor** × **Hello Time**, it considers the root bridge or the link to the root bridge to be faulty. **Time-factor** is a multiple of **Hello Time** and can be configured.
FWD Delay	2	Forwarding delay. This time parameter controls the duration of listening and learning states.
Ver 1 Length	1	The value is 0x00, indicating that the BPDU does not contain content of Version 1. STP does not have this field.

3. Port Roles

RSTP uses alternate ports and backup ports to replace blocking ports, and adds the edge port auto-identification function. Therefore, RSTP supports six types of ports:

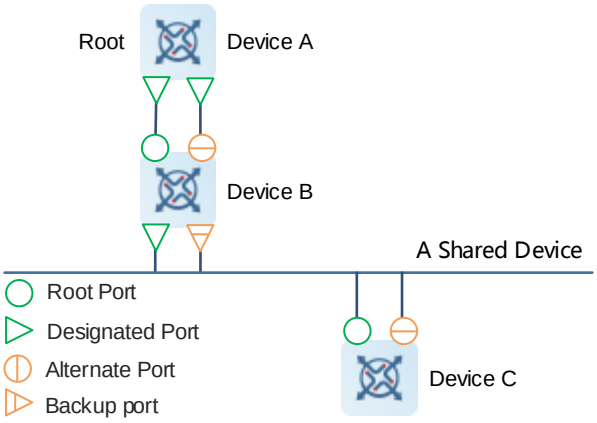
- Root port: A port with the shortest path to the root bridge.
- Alternate port: A backup port of a root port. Once the root port fails, the alternate port becomes the root port immediately.
- Designated port: A port that connects a root bridge or upstream bridge to a downstream device.
- Backup port: A backup port of a designated port. When a root bridge or upstream bridge has two interfaces to connect to the same downstream bridge, the interface with a higher priority is the designated port and the interface with a lower priority is the backup port. Once the designated port fails, the backup port becomes the designated port immediately.
- Edge port: A port connected to a terminal. Edge ports do not participate in spanning tree calculation. They can rapidly enter forwarding state with no need to wait for twice the period of **Forward Delay**. An edge port that receives a BPDU automatically becomes a non-edge port.
- Disable port: A port in down state.

Improvement effects:

- The work mechanism of the alternate port and backup port enables a device to restore the network connectivity within several milliseconds after discovering a topology change, with no need to transmit configurations.
- The status change of an edge port will neither affect the network connectivity nor cause loops. Edge ports can enter forwarding state without delay.

Figure 1-6 shows port roles. The port priority sequence is as follows unless otherwise specified: root port > designated port > alternate port > backup port.

Figure 1-6 RSTP Port Roles



4. BPDU Processing of RSTP

In RSTP, a device processes BPDUs in a different way.

- Independent Hello: After an STP topology becomes stable, the root bridge sends configuration BPDUs at an interval of **Hello Timer**. Non-root switches send configuration BPDUs only after receiving the configuration

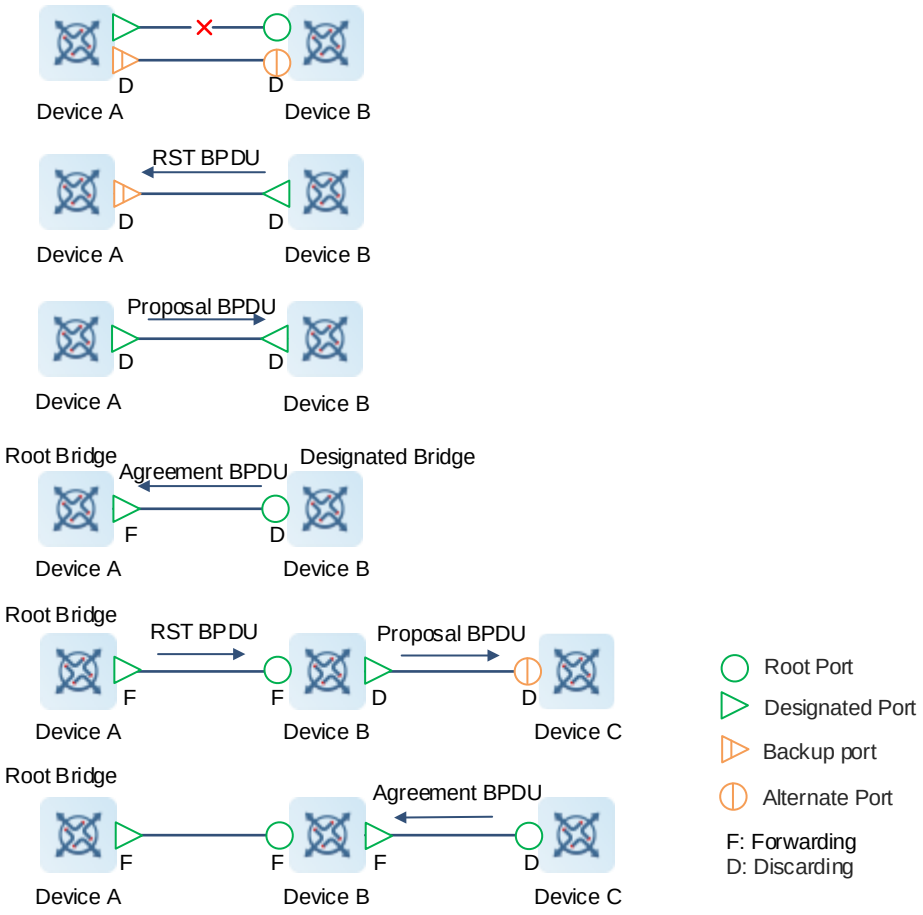
BPDU from the upstream device, resulting in long convergence time in the case of a topology change. After an RSTP topology is stable, non-root switches automatically send configuration BPDUs at an interval of **Hello Timer** regardless of whether they receive configuration BPDUs from the root bridge.

- Fast fault detection: In STP, if a non-root switch fails to receive a BPDU from the upstream device within one period of **MAX Age**, the switch considers the upstream device to be faulty. In RSTP, if a non-root switch fails to receive a BPDU from the upstream device within three periods of **Hello Time**, it considers the upstream device to be faulty. The value range of **Max Age** is from 6 to 40, in seconds, the default value is **20**, and it takes at least 6s to detect the upstream device fault. The value range of **Hello Time** is from 1 to 10, in seconds, the default value is **2**, and it takes at least 3s to detect the upstream device fault. Therefore, RSTP supports a shorter fault detection time.
- Fast convergence: In STP, all ports discard low-priority BPDUs upon receipt. If a blocking port fails to receive a high-priority BPDU within one period of **MAX Age**, the port changes to the designated port and sends its BPDU to the peer. In RSTP, when a downstream device receives a BPDU from the upstream device and finds that the priority of the BPDU is lower than that of the BPDU stored in the port, it sends its stored BPDU to the upstream device immediately. The upstream device compares the received BPDU with its own BPDU and updates the BPDU stored in the local port. This mechanism can accelerate topology convergence.

5. Fast Convergence of RSTP

In STP, to transition from listening state to learning state and then to forwarding state, a port needs to wait for two periods of **Forward Delay**. The value range of **Forward Delay** is from 4 to 30, in seconds, the default value is **15**, and therefore, the default waiting time is **30**s. In RSTP, a port enters discarding state after role election is complete, and then performs a Proposal/Agreement handshake with the connected bridge so as to quickly enter forwarding state. Figure 1-7 shows a fast convergence process of RSTP for example.

Figure 1-7 Fast Convergence of RSTP



(1) Proposal: If the root port of Device B fails to receive a BPDU from the upstream device within three periods of **Hello Time**, it considers the upstream device to be faulty. Device B returns to the initial state, considers itself as the root, and sets all its ports as designated ports (in discarding state) to send RST BPDUs. The alternate port (if Device A is not the root) or backup port (if Device A is the root) of Device A receives an RST BPDU from Device B. If Device A finds that the RST BPDU from Device B has a lower priority than its RST BPDU, Device A sets its port as a designated port (in discarding state), sets the **Proposal** bit in the configuration BPDU of the port to **1**, and sends a Proposal BPDU to Device B to request Device B to recognize Device A as the root bridge.

(2) Agreement: Device B receives the Proposal BPDU from Device A. If the BPDU of Device A is superior to that of Device B, Device B considers Device A as the root bridge (Device A may be the root or an intermediate device between Device B and the root). The port receiving the Proposal BPDU on Device B becomes the root port, and the root port stops sending RST BPDUs. Before a port transitions to forwarding state, Device B needs to block non-edge designated ports to prevent loops. The time required by ports to transition to -discarding state may be different. Devices use a set of synchronization variables to indicate whether the port state transition is complete. Device B sets the **Sync** variable to **1** for all ports. After all the ports enter discarding state, the **Synced** variable of all the ports is set to **1**. Then, the **Synced** variable of the root port is set to **1**, indicating that all the ports have been transitioned to the correct state. The root port sets the **Proposal** bit to **0** and the **Agreement** bit to **1** in the Proposal BPDU received from Device A and keeps other content of the BPDU unchanged, to create an Agreement BPDU. Then, the root port sends the BPDU to Device A.

(2) Forwarding: The designated port of Device A enters forwarding state after receiving the Agreement BPDU, and sends the RST BPDU with the **Forwarding** bit set to **1** at an interval of **Hello Time**. After receiving the RST BPDU, the root port of Device B enters forwarding state.

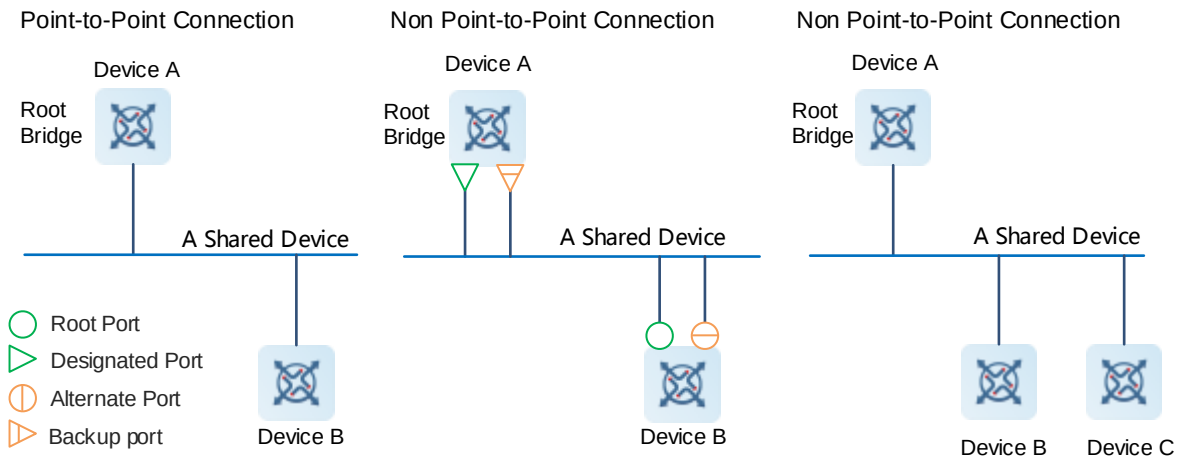
(3) Extension proposal: The designated port of Device B sends a Proposal BPDU with both **Proposal** and **Agreement** bits set to **1** to the downstream device, to request the downstream device to recognize Device B as the upstream device and extend the spanning tree. Theoretically, RSTP can recover the network tree topology immediately and achieve fast convergence once the network topology changes.

Improvement effect: Non-edge designated ports are blocked actively, without waiting for the period of **Forward Delay**. Hence, the convergence is accelerated. Network connectivity can be restored within the time of exchanging two handshake BPDUs, and the delay incurred by handshakes is less than 1s.

Caution

The above "handshake" process must meet one condition: Ports must be in a point-to-point connection state. Otherwise, the ports cannot shake hands and fast convergence cannot be achieved. To make RSTP-compliant devices function as they should, you are advised to connect devices in a point-to-point way.

Figure 1-8 Examples of Point-to-Point Connection and Non Point-to-Point Connection



6. Drawbacks of RSTP

- RSTP produces only one spanning tree in the whole switching network, which cannot prevent performance degradation caused by the network expansion. Therefore, when using RSTP, it is not recommended that the number of devices between any two nodes running STP/RSTP in the network exceed 7.
- RSTP can only implement redundant backup but does not support load balancing based on VLAN traffic.
- STP and RSTP calculate the spanning tree topology based on devices (nodes), and the impact of VLANs is not taken into account. In a particular topology, ports in the same VLAN may be blocked and fail to communicate with each other. This problem and the solution will be detailed in the MSTP section.

1.1.5 MSTP

1. Overview

MSTP, defined by the IEEE 802.1s standard, is capable of ironing out drawbacks of STP, RSTP (only one spanning tree is generated for a device), and Per-VLAN Spanning Tree (PVST) (one spanning tree is generated for each VLAN).

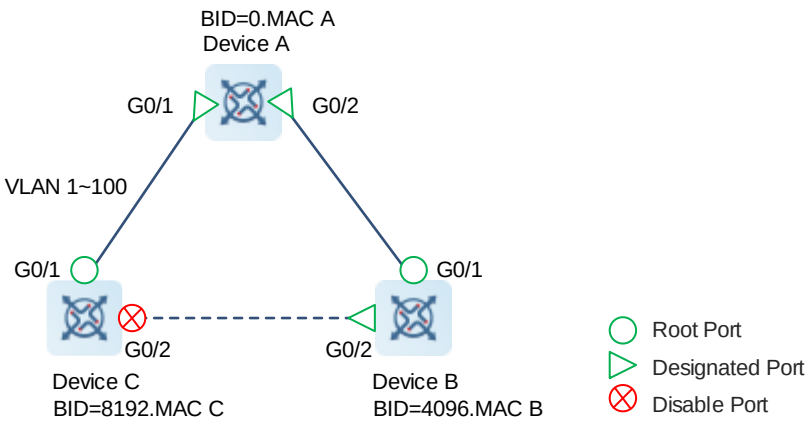
- After MSTP is deployed, if a loop arises in a network, MSTP performs topology calculation, and eliminates possible loops in the network by blocking redundant links.
- When an active path fails, MSTP activates the redundant backup link to restore the network connectivity.
- MSTP supports fast convergence.
- MSTP forwards the traffic of different VLANs along their respective spanning trees, which provides a better load balancing mechanism for redundant links.

2. Origin of MSTP

The conventional STP and RSTP protocols have the following two problems and MSTP emerges as a solution to them.

- Both STP and RSTP block redundant lines and concentrate traffic on the active link, which leads to a waste of bandwidth of the redundant link and heavy traffic on the active link, resulting in traffic imbalance.

Figure 1-9 Traffic Sharing Failure in STP

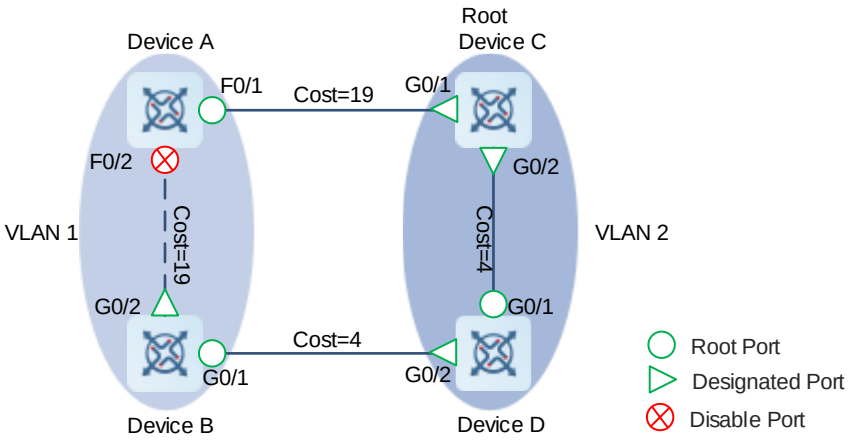


As shown in Figure 1-9, assume that the rate of each segment of link is 1 Gbps. If Devices A, B, and C run STP, the STP algorithm first elects Device A as the root based on the bridge ID. On non-root bridge B, the STP algorithm compares <**Root Path Cost**, **Bridge ID**, **Port ID**> in sequence, and selects port GigabitEthernet 0/1 as the designated port based on the root path cost. STP performs the same operation on Device C. Ports on the directly connected segment between Device C and Device B have the same root path cost. Port GigabitEthernet 0/2 of Device B is elected as the designated port based on the bridge ID, and port GigabitEthernet 0/2 of Device C is blocked. Port GigabitEthernet 0/2 of Device C cannot make communication due to STP blocking. VLANs 1–100 can be configured only on port GigabitEthernet 0/1 of Device C. It is impossible to implement traffic sharing by configuring port GigabitEthernet 0/1 of Device C to allow VLANs 1–50 and port GigabitEthernet 0/2 of Device C to allow VLANs 51–100.

- In special cases, STP and RSTP may block links in the same VLAN, causing interfaces within the same

VLAN to be unable to communicate with each other.

Figure 1-10 Communication Failure in the Same VLAN Caused by STP



As shown in Figure 1-10, Devices A and B are in VLAN 1, and Devices C and D are in VLAN 2. Assume that the topology tree calculated by STP is shown in the figure. Port FastEthernet 0/2 of Device A is blocked, and the link between Devices A and B is blocked. VLAN 1 is not configured on Devices C and D, and Devices C and D cannot forward packets of VLAN 1. As a result, Devices A and B in VLAN 1 cannot communicate with each other.

3. Instance and Instance Mapping

The collection of one or more VLANs on one device is called a Multiple Spanning Tree Instance (MSTI) or instance for short. If a device supports a maximum of 65 instances, instance **0** exists by default and cannot be deleted, and instances 1–64 can be created or deleted. Users can allocate VLANs 1–4094 to different instances as required, and unallocated VLANs belong to instance **0** by default. The mapping between MSTIs and VLANs is called instance mapping, as shown in Table 1-9.

Table 1-9 Mappings Between MSTIs and VLANs

Instance	VLAN Mapped
0	1–2, 4, 11–4094
1	3, 5–7
2	8–10

Note

You are advised to disable MSTP before configuring mappings between MSTIs and VLANs, and then enable MSTP after configuration, to ensure stable convergence of the network topology.

4. Multiple Spanning Tree Region

Devices that run the MSTP protocol, have the same configuration name, revision number, and instance mappings constitute a multiple spanning tree (MST) region. Configuration names, revision numbers, and instance mappings are recorded in the **MST CFG ID** field of MST BPDUs and they can be configured.

- Configuration name: A string of 32 bytes used to identify an MST region.
- Revision number: A 2-byte non-negative integer used to identify an MST region.
- Instance mapping: The mappings between MSTIs and VLANs are encrypted into a 16-byte digest. One MST region can contain multiple MSTIs.

MST regions are independent of each other. If a port on a device receives a BPDU with **MST CFG ID** same as that of the MST BPDU of the device, the device deems that the peer device and the device belong to the same MST region. Otherwise, the device deems that the peer device belongs to a different MST region. The load sharing advantage of MSTP can be reflected only after multiple devices are configured to the same MST region. Therefore, MST regions need to be properly divided and devices in the same MST region need to have the same **MST CFG ID**.

5. Instance Spanning Tree

One instance spanning tree can be generated for each instance. Each instance calculates and generates an instance spanning tree based on MSTI configuration messages in MST BPDUs. Information contained in MST configuration messages is described in Table 1-10.

If a device contains only one instance or MST configuration messages of multiple instances are the same, the same instance spanning tree will be generated, which is useless in traffic sharing. If VLANs are allocated to different instances to form multiple VLAN groups and different bridge priorities and port priorities are configured for different instances, multiple different instance spanning trees can be generated for the instances in the region to share VLAN traffic. The spanning tree of each instance is not affected by the spanning trees of other instances.

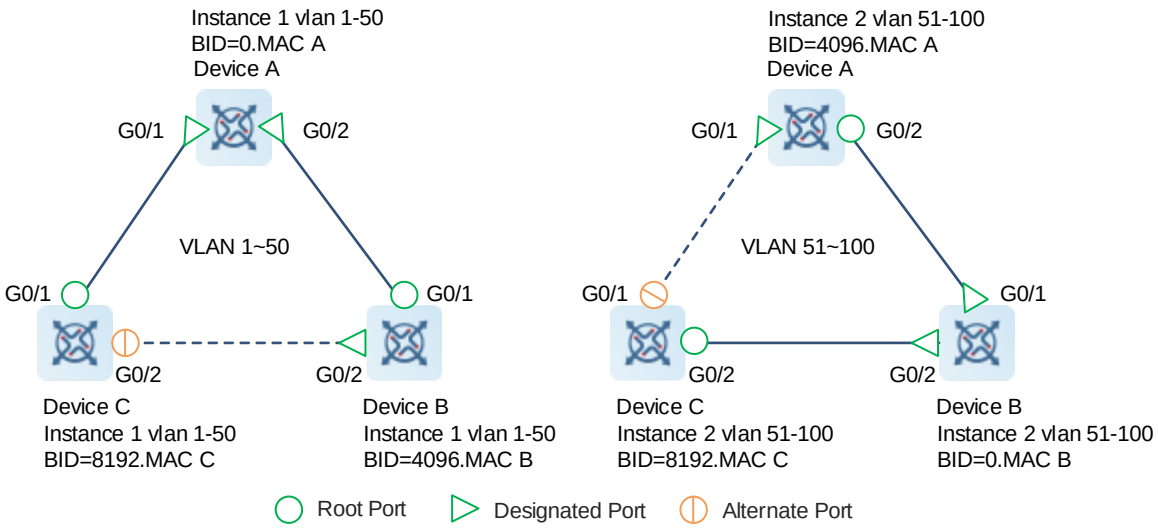
Caution

"MSTI configuration messages" of instances need to be manually modified so that spanning trees of instances are different, that is, the selected root, designated ports, blocking ports, and active links are different for different instances. In this way, VLAN traffic sharing can come into play.

MSTP calculates the topology for each instance in the same way as RSTP. In each instance, MSTP first elects the root bridge by comparing the root ID, and all ports on the root bridge are designated ports. Then, MSTP compares key elements in the priority vector <**Root ID**, **Root Path Cost**, **Bridge ID**, **Port ID**> on non-root bridges to elect root ports. Afterwards, MSTP compares the two ports of each directly connected network segment, and elects the port with a higher priority as the designated port and the one with a lower priority as the alternate port. Devices produce multiple instance spanning trees by means of MST BPDU interaction and calculation. Each instance provides a single loop-free network topology for VLAN groups in the instance, and the topologies of different VLAN groups are different.

For example, after MSTP runs in the topology as shown in Figure 1-9, the calculated topology is shown in Figure 1-11.

Figure 1-11 Traffic Sharing Implemented by MSTP



In instance 1, devices elect Device A as the root by comparing root IDs (bridge IDs of the devices at this moment). Devices compare the root path cost and elect port GigabitEthernet 0/1 of Device B and port GigabitEthernet 0/1 of Device C as the root ports. In the directly connected network segment between Devices C and B, the two devices have the same root ID (0.MAC A). Bridge ID of Device B is smaller than that of Device C, and therefore, port GigabitEthernet 0/2 of Device B is elected as the designated port and port GigabitEthernet 0/2 of Device C is elected as the alternate port. When port GigabitEthernet 0/1 of Device C malfunctions, port GigabitEthernet 0/2 of Device C becomes the root port immediately.

In instance 2, devices elect Device B as the root by comparing root IDs (bridge IDs of the devices at this moment). Devices compare the root path cost and elect port GigabitEthernet 0/2 of Device A and port GigabitEthernet 0/2 of Device C as the root ports. In the directly connected network segment between Devices A and C, the two devices have the same root ID (0.MAC B). Bridge ID of Device A is smaller than that of Device C, and therefore, port GigabitEthernet 0/1 of Device A is elected as the designated port and port GigabitEthernet 0/1 of Device C is elected as the alternate port. When port GigabitEthernet 0/2 of Device C malfunctions, port GigabitEthernet 0/1 of Device C becomes the root port immediately.

It can be seen that different spanning trees are calculated for instance 1 and instance 2 due to different bridge IDs. Consequently, packets of VLANs 1–50 are forwarded along the spanning tree of instance 1 and packets of VLANs 51–100 are forwarded along the spanning tree of instance 2, implementing VLAN traffic sharing.

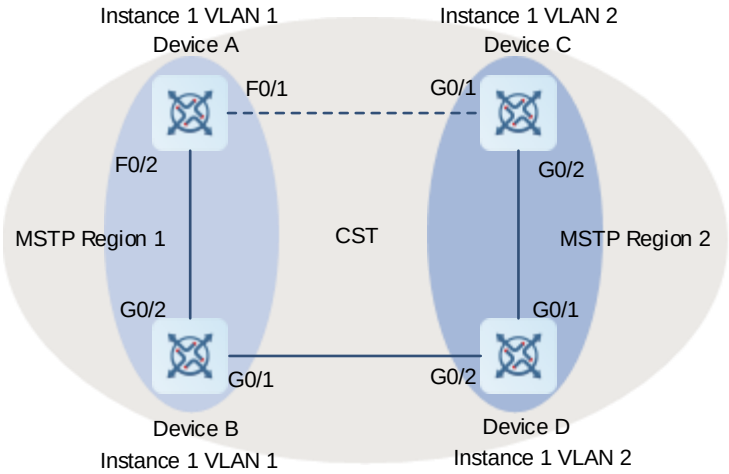
Users can, as needed, configure different instances for different VLAN groups, Configuring the Bridge Priority and Port Priority by instance, Configuring the Port Path Cost, and plan VLAN groups to forward traffic through different paths.

6. Common Spanning Tree

Devices with different instances and VLAN mapping configurations do not belong to the same MST region and each MST region is a whole. Therefore, one MST region can be considered as one node. The inter-node spanning tree calculated via STP is called a common spanning tree (CST). Instances with the same ID can exist in different MST regions, for example, instance 1 exists in two MST regions. Though the instance IDs are the same, instance spanning trees are generated independently for the instances and the instances are

unrelated to each other and unrelated to the CST. If two MST regions are configured in a topology shown in Figure 1-10, the calculated topology is shown in Figure 1-12 after MSTP runs.

Figure 1-12 Preventing a Communication Failure of Ports in the Same VLAN by MSTP



Devices A and B (both instance 1 VLAN 1) have the same instance mapping. There is no loop in MST region 1, and therefore, no port is blocked in this region.

Devices C and D (both instance 1 VLAN 2) have the same instance mapping. There is no loop in MST region 2, and therefore, no port is blocked in this region.

MST region 1 and MST region 2 can be considered as two nodes and there are loops between the two nodes. Therefore, a link is blocked according to the configuration to prevent loops and ensure that the intra-VLAN communication is not affected.

7. Common and Internal Spanning Trees

In a topology as shown in Figure 1-13, there are three MST regions. In each MST region, one instance spanning tree is generated for each instance. As shown in Figure 1-14, in region 2, one spanning tree is generated for instance 0, instance 1, and instance 2 each. According to the MSTP protocol, the spanning tree of instance 0 represents the region and is called an internal spanning tree (IST).

Each MST region is considered as a node, and one spanning tree is calculated between nodes according to the STP protocol. This spanning tree is called a common spanning tree (CST). As shown in Figure 1-13, a spanning tree connected using blue lines indicates an IST in a region while a spanning tree connected using orange lines indicates an inter-region CST.

ISTs and a CST constitute a common and internal spanning tree (CIST).

CIST root: Root of a CIST. It is also the root of a CST, that is, CST root. In the CST calculation, the device with the smallest bridge ID is elected as the CIST root. As shown in Figure 1-13, assume that Device A has the smallest bridge ID. Device A is elected as the CIST root.

Region root: In an IST, the device with the smallest root path cost to the CIST root is elected as the region root of the IST, which is also called master bridge. CIST root A is also the region root of region 1. As shown in Figure 1-13, assume that Device B in region 2 has the smallest root path cost to Device A. Device B is elected as the region root of region 2. Device B may not be directly connected to Device A but may through other devices in region 1. Likewise, Device C is elected as the region root of region 3.

The region root of region 2 is Device B. Suppose that three spanning trees are calculated for the three instances in region 2, and the roots of the three spanning trees are all Device B. On Device B, the port with the smallest root path cost to the CIST root is the master port. Therefore, compared with RSTP, MSTP adds two port roles: master port and region edge port.

Caution

The **CIST Regional Root** field in MSTP packets indicates a region root rather than the CIST root.

A region root (represented by **CIST Regional Root**) may not be the device with the smallest bridge ID in a region but is the device with the smallest root path cost from the region to the CIST root.

To make the topology more stable, it is recommended that the "outlets" of different instance spanning trees in each region to the CIST root be configured on the same device of the region. As shown in Figure 1-14, the outlets of MSTI 1, MSTI 2, and MSTI 3 in region 2 to the CIST root are configured on Device B.

Figure 1-13 CIST Composed of ISTs and the CST

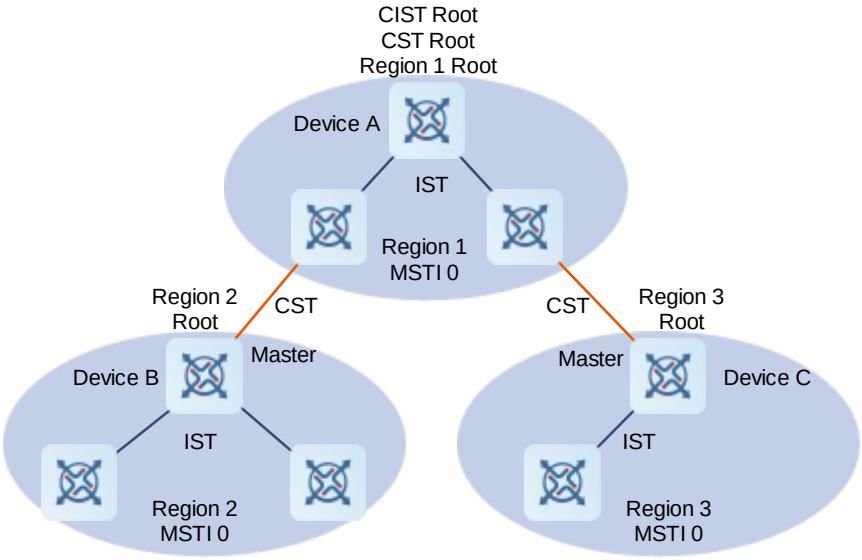
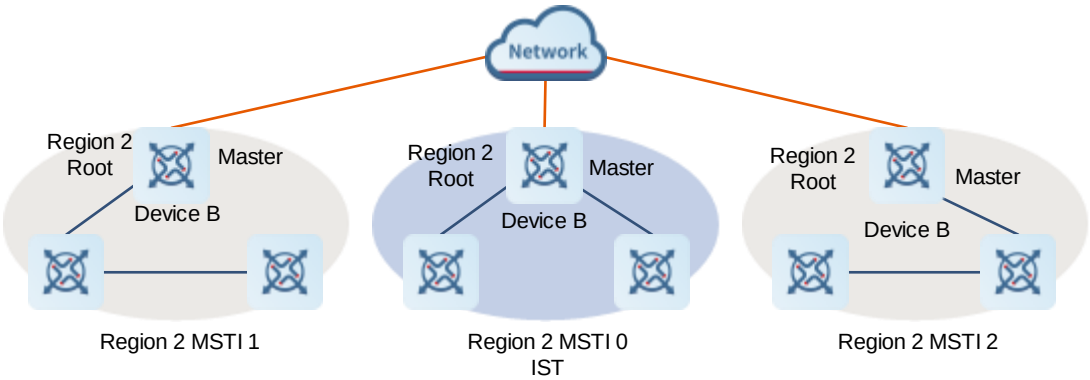


Figure 1-14 Three Spanning Trees Generated for the Three Instances in Region 2



8. Port Roles

MSTP introduces a new port role to the region root: master port, which is the port with the smallest root path cost from a region to the CIST root. The master port is the "outlet" of all instances in a region, and all instances can forward data through the master port.

- Root port: A port with the shortest path to the root bridge.
- Designated port: A port that connects a bridge to the root bridge in each LAN.
- Alternate port: A backup of a root port. Once the root port fails, the alternate port becomes the root port immediately.
- Backup port: A backup of a designated port. When two ports on a bridge connect to the same LAN, the port with a higher priority is the designated port and the one with a lower priority is the backup port. Once the designated port fails, the backup port changes to the designated port immediately.
- Edge port: A port connected to a terminal. Edge ports do not participate in spanning tree calculation.
- Disable port: A port in down state.
- Master port: A port with the shortest path cost to the CIST root. It is the "outlet" of all MSTIs in an MST region.
- Region edge port: A port directly connected to other MST regions. A master port is a special region edge port.

9. MSTP Packets

MSTP uses MST BPDUs as the basis for spanning tree calculation. MST BPDUs can be used to calculate spanning tree topologies, maintain network topologies, and communicate topology change records.

Figure 1-15 Configuration BPDU of MSTP

```
0000  01 80 c2 00 00 00 00 d0  f8 22 35 4a 00 69 42 42
0010  03 00 00 03 02 7c 80 00  00 d0 f8 22 35 4a 00 00
0020  00 00 80 00 00 d0 f8 22  35 4a 80 1c 00 00 14 00
0030  02 00 0f 00 00 00 40 00  00 00 00 00 00 00 00 00
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0050  00 00 00 00 00 00 00 00  00 00 ac 36 17 7f 50 28
0060  3c d4 b8 38 21 d8 ab 26  de 62 00 00 00 00 80 00
0070  00 d0 f8 22 35 4a 14
```

As shown in Figure 1-15, the **Length** field is 0x0069, which indicates that the packet length is 105 bytes in this example, including a 3-byte LLC header and a 102-byte MST BPDU. This length is the minimum length of an MST BPDU. For both intra-region and inter-region MST BPDUs, the first 36 bytes are the same as those of an RST BPDU. MSTP-specific fields start from the 37th byte, and the MSTI configuration message field at the end is composed of multiple MSTI configuration messages. The fields are described in Table 1-10.

Table 1-10 Format of an MST BPDU

Field	Bytes	Description
PID	2	Protocol identifier. The value is 0x0000.
PVID	1	Protocol version identifier. 0x03 indicates that the packet protocol is MSTP.
BPDU Type	1	BPDU packet type. The value is 0x02 for MSTP. 0x02 indicates that the BPDU type is MST BPDU.

CIST Flags	1	Configuration BPDUs of MSTP use all the eight bits. In the example, the value is 0x7c, that is, 0111 1100.
		● Bit 7: TCA. An upstream device sets bit 7 in a configuration BPDU to **1** and sends the BPDU to notify the downstream device of the topology change and request the downstream device to stop sending the TCN BPDU.
		● Bit 6: Agreement. The value **1** indicates consent to status switching.
		● Bit 5: Forwarding. The value **1** indicates forwarding state.
		● Bit 4: Learning. The value **1** indicates learning state.
		● Bit 3 and bit 2: Port role.
		  ○ 00: Unknown.
		  ○ 01: Root port.
		  ○ 10: Alternate/Backup.
		  ○ 11: Designated port.
		● Bit 1: Proposal. The value **1** indicates sending a proposal to request status switching.
		● Bit 0: TC. The root bridge sets bit 0 in a configuration BPDU to **1** and sends the BPDU to instruct the downstream device to delete MAC address entries.

CIST Root ID	8	Bridge ID of the CIST root, which consists of a 2-byte root priority and a 6-byte root MAC address. In the example, the priority value is 0x8000, which indicates 32768, and the bridge MAC address is 00-d0-f8-22-35-4a.
CIST External Path Cost	4	CIST external path cost, which refers to the cumulative path cost from the MST region, to which the device belongs, to the CIST root. The CIST external path cost is calculated based on the link bandwidth, which is 0x00 00 00 00 in the example.
CIST Regional Root ID	8	CIST regional root identifier, that is, bridge ID of the IST master bridge. If the CIST root is in the region, the region root ID is the CIST root ID. In the example, the priority value is 0x8000, which indicates 32768, and the bridge MAC address is 00-d0-f8-22-35-4a.
CIST Port ID	2	ID of a port in an IST. In the example, the priority value is 0x80, which indicates 128, and the port ID is 1c.

Field	Bytes	Description
Message Age	2	Age of a BPDU, that is, keepalive time of the packet. The value is 0x0000 in the example.
Max Age	2	Maximum timeout time of a BPDU, after which the link to the root switch is considered to be faulty. The value in the example is 0x1400 (low-order bytes on the left), indicating 20 seconds.
Hello Time	2	Hello interval for sending two adjacent BPDUs. The default value is **2**s. The value in the example is 0x0200 (low-order bytes on the left), indicating 2 seconds.
FWD Delay	2	**Forward Delay** timer. The default value is **15**s. This field controls the duration of listening and learning states. The value in the example is 0x0f00 (low-order bytes on the left), indicating 15 seconds.
Ver 1 Length	1	Length of a Version1 BPDU. The value is fixed to 0x00.
Ver 3 Length	2	Length of a Version3 BPDU. The value is 0x0040 in the example.
MST CFG ID	51	MST configuration identifier, that is, MST region label information, which contains four fields. Interconnected devices with the same four fields in **MST CFG ID** belong to the same region. ● (1-byte) Configuration Identifier Format Selector: The value is fixed to 0x00. ● (32-byte) Configuration Name: Region name. The default value is all 0's. ● (2-byte) Revision Level: Revision number, which is a non-negative integer. The value is 0x0000. ● (16-byte) Configuration Digest: MSTI-VLAN instance mapping table. The HMAC-MD5 algorithm is used to encrypt the mappings between instances and VLANs in a region into a 16-byte digest.
CIST Internal RPC	4	CIST internal root path cost, which is the cumulative path cost from the local port to the master switch of the IST. The internal root path cost of a CIST is calculated based on the link bandwidth. The value is 0x00-00-00-00 in the example.
CIST Bridge ID	8	ID of the designated switch in the CIST. It consists of a 2-byte bridge priority and a 6-byte bridge MAC address. In the example, the priority value is 0x8000, which indicates 32768, and the bridge MAC address is 00-d0-f8-22-35-4a.
CIST R Hops	1	Number of remaining hops of a BPDU in a CIST. The default value is 0x14, which indicates 20 hops.

Field	Bytes	Description
MSTI Configuration Messages (may be absent)	16	MSTI configuration message. The configuration message of each MSTI occupies 16 bytes. If there are *n* MSTIs, they occupy *n* × 16 bytes. Fields in the configuration message of a single MSTI are described as follows: ● (1-byte) MSTI Flags: MSTI flag. ● (8-byte) MSTI Regional Root Identifier: MSTI region root ID. ● (4-byte) MSTI Internal Root Path Cost: Cumulative path cost from the local port to the MSTI region root switch. The internal root path cost of an MSTI is calculated based on the link bandwidth. ● (1-byte) MSTI Bridge Priority: Bridge priority of the device in the MSTI. ● (1-byte) MSTI Port Priority: Port priority of the device in the MSTI. ● (1-byte) MSTI Remaining Hops: Number of remaining hops of a BPDU in the MSTI.

1.1.6 Protocols and Standards

- IEEE 802.1D: Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
- IEEE 802.1w: IEEE Standard for Information Technology -Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Common Specifications - Part 3: Media Access Control (MAC) Bridges:Amendment 2:Rapid Reconfiguration
- IEEE 802.1s: IEEE Standards for Local and Metropolitan Area Networks - Amendment to 802.1Q Virtual Bridged Local Area Networks: Amendment 3: Multiple Spanning Trees

1.2 Configuration Task Summary

1.2.1 Configuring STP

The STP basic configuration includes the following tasks:

(1) Configuring the Spanning Tree Mode

(2) (Optional) Configuring the Bridge Priority and Port Priority

(3) (Optional) Configuring the Port Path Cost. Select at least one of the following to configure.

- Configuring the Path Cost Calculation Method
- Configuring the Path Cost Value

(4) (Optional) Configuring Spanning Tree Time Parameters

(5) Enabling the STP Function

1.2.2 Configuring RSTP

The RSTP basic configuration includes the following tasks:

(1) Configuring the Spanning Tree Mode

(2) (Optional) Configuring the Bridge Priority and Port Priority

(3) (Optional) Configuring the Port Path Cost. Select at least one of the following to configure.

- Configuring the Path Cost Calculation Method
- Configuring the Path Cost Value

(4) (Optional) Configuring Spanning Tree Time Parameters

(5) (Optional) Configuring Fast Convergence of Spanning Trees

(6) (Optional) Enabling Protocol Migration

(7) Enabling the STP Function

1.2.3 Configuring MSTP

The MSTP basic configuration includes the following tasks:

(1) Configuring the Spanning Tree Mode

(2) Configuring an MST Region

(3) Configuring the Bridge Priority and Port Priority

(4) (Optional) Configuring the Port Path Cost. Select at least one of the following to configure.

- Configuring the Path Cost Calculation Method
- Configuring the Path Cost Value

(5) (Optional) Configuring Spanning Tree Time Parameters

(6) (Optional) Configuring the Maximum Hop Count for BPDUs

(7) (Optional) Configuring Fast Convergence of Spanning Trees

(1) (Optional) Configuring Spanning Tree Compatibility for Interfaces

(2) Enabling the STP Function

1.2.4 Configuring Advanced Functions for Spanning Trees

Configuring advanced functions for spanning trees includes the following tasks. In networking applications, these functions are used to enhance the stability, robustness, and anti-attack capability of protocols based on the network topology and application characteristics, so as to meet the application requirements of protocols in different user scenarios. The following configuration tasks are all optional. When performing the following configuration, be sure to complete the configuration and then enable spanning tree protocols.

- Configuring Port Protection
  - Configuring Root Guard
  - Configuring Loop Guard
- Configuring BPDU Source MAC Address Check
- Configuring an Edge Port
  - Configuring Autoedge
  - Configuring the Port Fast Attribute
- Configuring BPDU Guard or BPDU Filter
  - Configuring BPDU Guard
  - Configuring BPDU Filter

- Configuring TC Attack Defense Functions
  - Configuring TC Protection
  - Configuring TC Guard
  - Configuring TC Filter
- Configuring BPDU Tunnel

1.2.5 Configuring BPDU Transparent Transmission

When STP/RSTP/MSTP is not enabled on a device, if the spanning tree between the device and the interconnected device needs to be calculated properly, BPDU transparent transmission needs to be configured on the device to transparently transmit BPDU frames.

- Configuring BPDU Transparent Transmission

1.3 Configuring the Spanning Tree Mode

1.3.1 Overview

According to IEEE 802.1 protocol standards, STP, RSTP, and MSTP are mutually compatible, without any configuration by the administrator. Some vendors' devices may not implement STP/RSTP/MSTP according to protocol standards, causing incompatibility. Therefore, Ruijie provides a spanning tree mode configuration command for the administrator to switch the spanning tree mode to a lower version if other vendors' devices are incompatible with a Ruijie device.

1.3.2 Restrictions and Guidelines

- **mstp** indicates the Multiple Spanning Tree Protocol (IEEE 802.1s).
- **rstp** indicates the Rapid Spanning Tree Protocol (IEEE 802.1w).
- **stp** indicates the Spanning Tree Protocol (IEEE 802.1d).
- If the STP mode is switched to RSTP mode, the convergence time is the convergence time of STP at the first topology change and the convergence time of RSTP at the second topology change.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the spanning tree mode.

spanning-tree mode { **mstp** | **rstp** | **stp** }

The default spanning tree mode is MSTP.

1.4 Configuring an MST Region

1.4.1 Overview

This section describes how to configure an MST region to change device members in the MST region, so as to affect the spanning tree topology.

1.4.2 Restrictions and Guidelines

- To enable multiple devices to belong to the same MST region, you need to configure the same configuration name, revision number, and instance mappings for the devices.
- One VLAN belongs to only one instance. All VLANs belong to instance **0** by default. In MST configuration mode, you can run the **instance vlan** command to move a VLAN group to an instance. For example, the **instance** 1 **vlan** 2-200 command moves VLANs 2–200 to instance **1**. The **instance** 1 **vlan** 2,20,200 command moves VLANs 2, 20, and 200 to instance **1**.
- You can run the **no instance vlan** command to move a VLAN from a custom instance to instance **0**.
- *instance-id* indicates an MST instance ID. The value range is from 0 to 64. *vlan-range* indicates a VLAN ID range. The value range is from 1 to 4094. It can be configured in MST configuration mode.
- *name* indicates an MST name, which can contain 32 bytes at most. The default value is an empty string.
- *version* indicates the MST revision number. The default value is **0** and the value range is from 0 to 65535.

1.4.3 Prerequisites

Only MSTP supports instance configuration. If the spanning tree mode is incorrect, run the **spanning-tree mode mstp** command to set the spanning tree mode to MSTP first.

You are advised to configure instance-VLAN mappings when STP is disabled, to ensure the stability and convergence of the network topology. If STP has been enabled, run the **no spanning-tree** command to disable STP. Enable STP only after completing the instance-VLAN mapping configuration.

1.4.4 Procedure

(1) Create VLANs.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a group of VLANs.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure instance-VLAN mappings.

a Enter the MST configuration mode.

spanning-tree mst configuration

b Add the VLAN group to an MST instance.

instance *instance-id* **vlan** *vlan-range*

Only instance **0** exists and all VLANs belong to instance **0** by default.

(3) (Optional) Configure a name of an MST region.

name *name*

The default name of an MST region is empty.

(4) (Optional) Configure a revision number for the MST region.

revision *version*

The default revision number of an MST region is **0**.

1.5 Configuring the Bridge Priority and Port Priority

1.5.1 Overview

The bridge priority concerns the root bridge election as well as the topology of the entire network. Configure the bridge priority when the administrator needs to change the root or topology of a network.

The port priority concerns the port role election as well as ports entering forwarding state. Configure the port priority when the administrator needs to change ports entering forwarding state. If a loop arises in a region, the port with a higher priority is preferentially selected to transition to forwarding state. When ports share the same priority, the port with a smaller port ID is selected to transition to forwarding state.

1.5.2 Restrictions and Guidelines

- The value range of an instance ID is from 0 to 64 and the default value is **0**.
- The options of bridge priority indicated by **priority** include 16 values, which are multiples of 4096, that is, 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. The default value is **32768**. It is recommended that the administrator configure a smaller bridge priority for core devices to ensure the network stability. Different bridge priorities can be configured for different instances, and each instance runs an independent STP based on the configuration. Devices in different regions care about the priority of only instance 0.
- The options of **port-priority** include 16 values, which are multiples of 16, that is, 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. The default value is **128**. Different port priorities can be configured for different instances on the same port, and an independent spanning tree can be generated for each instance based on the configuration. The changed port priority takes effect only if the port priority is changed on designated ports.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the bridge priority.

- In STP/RSTP mode, configure the bridge priority.

spanning-tree priority *priority*

The default bridge priority is **32768**.

- In MSTP mode, configure the bridge priority for a specified instance.

  spanning-tree mst *instance-id* **priority** *priority*

  The default bridge priority is **32768**.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure the port priority.

- In STP/RSTP mode, configure the port priority.

  spanning-tree port-priority *port-priority*

  The default port priority is **128**.

- In MSTP mode, configure the port priority for a specified instance.

  spanning-tree mst *instance-id* **port-priority** *port-priority*

  The default port priority is **128**.

1.6 Configuring the Port Path Cost

1.6.1 Overview

The port path cost determines the root port election result on a device. A device elects the port with the minimum root path cost as the root port. The root path cost is the sum of path costs of all ports in the path from a device to the root.

The port path cost also affects the BPDU priority as well as the overall network topology. When devices compare the BPDU priority, the root path cost is compared if BPDUs have the same root ID and bridge ID.

The administrator can configure the port path cost to determine the port or path, through which packets pass preferentially. You can manually configure the port path cost by modifying the method of calculating the default path cost or directly specifying the path cost.

1.6.2 Restrictions and Guidelines

By default, the port path cost is automatically calculated based on the interface link rate. A higher link rate indicates a lower path cost and vice versa. With this calculation method, devices can calculate the optimal spanning tree topology. You are not advised to modify the path cost unless otherwise indicated.

1.6.3 Configuration Tasks

The configuration includes the following tasks:

(1) Configuring the Path Cost Calculation Method

(2) Configuring the Path Cost Value

1.6.4 Configuring the Path Cost Calculation Method

1. Overview

If no specific path cost is configured, the device automatically calculates the port path cost based on the physical port rate by using the calculation method stipulated in the standard. The administrator can modify the method of automatically calculating the port path cost for a device so that the device calculates different port path cost values.

2. Restrictions and Guidelines

- Be sure to adopt a consistent port path cost standard for the entire network.
- IEEE 802.1d Short: The range of the port path cost is from 1 to 65535. Aggregate port cost = Physical port cost × 95%.
- IEEE 802.1t Long: The range of the port path cost is from 1 to 200000000. Aggregate port cost = Physical port cost × 95%.
- IEEE 802.1t Long Standard: The range of the port path cost is from 1 to 200000000. Aggregate port cost = Physical port cost/Linkupcnt. At this moment, the cost value of the aggregate port will change with the number of member ports, which will lead to the network topology change. For configurations of aggregate ports and the Link Aggregation Control Protocol (LACP), see *Configuring Aggregate Port*.
  - When an aggregate port is a static aggregate port, **Linkupcnt** refers to the number of member ports in Link Up state.
  - When an aggregate port is an LACP aggregate port, **Linkupcnt** refers to the number of member ports participating in the aggregate port data forwarding.
  - When no member port of an aggregate port is in Link Up state or forwarding data, the value of **Linkupcnt** is **1**.

Table 1-11 Port Path Costs Calculated Based on the Link Rate

Port Rate	Port	IEEE 802.1d Short	IEEE 802.1t Long	IEEE 802.1t Long Standard
10 Mbps	Common port	100	2000000	2000000
	Aggregate port	95	1900000	2000000/Linkupcnt
100 Mbps	Common port	19	200000	200000
	Aggregate port	18	190000	200000/Linkupcnt
1000 Mbps	Common port	4	20000	20000
	Aggregate port	3	19000	20000/Linkupcnt
10000 Mbps	Common port	2	2000	2000
	Aggregate port	1	1900	20000/Linkupcnt

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Modify the automatic calculation method.

spanning-tree pathcost method { **long** | **long standard** | **short** }

The port path cost is calculated according to IEEE 802.1t Long by default.

1.6.5 Configuring the Path Cost Value

1. Overview

You can manually specify the port path cost. After configuration, the port path costs automatically calculated based on the physical port rate are not used.

2. Restrictions and Guidelines

- In MSTP application, you can configure different path costs for different instances on an interface so that different instance spanning trees are generated for the instances to implement load sharing.
- **mst** *instance-id*: Specifies the instance ID. The value range is from 0 to 64 and the default value is **0**.
- **cost** *cost*: Specifies the path cost value. The value range is from 1 to 200000000. The path cost value is automatically calculated based on the link rate of a port by default. A larger value of *cost* indicates a greater path cost.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(1) Enter the global configuration mode.

configure terminal

(2) Enter the interface configuration mode.

interface *interface-type interface-number*

(3) Configure the port path cost.

- In STP/RSTP mode, configure the port path cost.

  spanning-tree cost *cost*

  The port path cost is calculated based on the port rate by default.

- In MSTP mode, configure the port path cost for a specified instance.

  spanning-tree mst *instance-id* **cost** *cost*

  The port path cost is calculated based on the port rate by default.

1.7 Configuring Spanning Tree Time Parameters

1.7.1 Overview

The timer in STP affects the spanning tree election and recovery performance.

Multiple parameters cannot be configured in one command at the same time. Only one of the following time parameters can be carried in the **spanning-tree** command:

- Interval for entering forwarding state (**Forward Time**)
- BPDU transmission interval (**Hello Time**)
- BPDU expiration time (**Max Age**)
- Number of BPDUs sent per second (**TX Hold Count**)
- Spanning tree timeout factor (**Factor**)

1.7.2 Restrictions and Guidelines

- **forward-time** *forward*: Specifies the port status change interval, in seconds. It refers to the interval for a port to transition from listening state to learning state or from learning state to forwarding when STP runs on a device or RSTP runs in STP compatible mode. It indicates the delay in the port status change. The value range is from 4 to 30, and the default value is **15**. If **Forward Delay** is too small, a temporary loop may occur. If **Forward Delay** is too large, the network recovery time may be very long.
- **hello-time** *hello*: Indicates the interval for the device to send BPDUs, in seconds. The value range is from 1 to 10, and the default value is **2**. If **Hello Time** is too small, the resource consumption of the device and network may increase. If the value is too small, the downstream device may mistakenly consider the uplink to be faulty, especially when packet loss occurs occasionally.
- **max-age** *age*: Indicates the maximum expiration time of BPDUs, in seconds. When the time expires, BPDUs will be discarded. The value range is from 6 to 40, and the default value is **20**. If **Max Age** is too small, link congestion may be wrongly judged as a link fault and the spanning tree is calculated very frequently. If the value is too large, the link fault cannot be found in time, resulting in poor network auto-recovery capability.

  Each device running STP or RSTP is a separate region, and is not allocated to a region with any other devices. Though MSTP uses the hop count mechanism to represent the lifecycle of BPDUs, the **Message Age** and **Max Age** mechanisms are still retained in order to be compatible with STP and RSTP outside regions.
- The value ranges of **forward-time, hello-time, and max-age** are related. Changing one of them will affect the value ranges of the other two parameters. Their restrictive relationship is as follows: 2 × (Hello Time + 1s) ≤ Max Age ≤ 2 × (Forward Delay – 1s). The configured three parameters must meet this condition. Otherwise, the topology may be unstable. In addition, the three parameters need to match the network size. A larger network diameter needs larger values of the parameters. You are advised to adopt automatic calculation according to the protocol to avoid manual configuration.
- **tx-hold-count** *count*: Configures the maximum number of BPDUs that can be sent per second. The value range is from 1 to 10 and the default value is **3**.
- **timer-factor** *factor*: Configures the packet receiving timeout factor. Timeout time = Timeout factor (indicated by *factor*) × Hello Time. If a device fails to receive a BPDU from the upstream device within the timeout time,

the spanning tree is re-calculated. The value range is from 1 to 30, and the default value is **3**.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the interval for the status change of a spanning tree port.

spanning-tree forward-time *forward*

The default interval for transitioning to forwarding state is 15s.

(4) Configure the interval for a spanning tree port to send BPDUs.

spanning-tree hello-time *hello*

The default interval for sending BPDUs is 2s.

(5) Configure the maximum number of BPDUs that can be sent by a spanning tree port.

spanning-tree tx-hold-count *count*

Three BPDUs are sent per second by default.

(6) Configure the maximum timeout time of spanning tree BPDUs.

spanning-tree max-age *age*

The default expiration time of BPDUs is 20s.

(7) Configure the spanning tree timeout factor.

spanning-tree timer-factor *factor*

The default spanning tree timeout factor is 3.

1.8 Configuring the Maximum Hop Count for BPDUs

1.8.1 Overview

MST regions do not use the **Message Age** and **Max Age** mechanisms to calculate whether BPDUs time out but use the maximum hop count mechanism for calculation. The maximum hop count mechanism is similar to the Time to Live (TTL) of IP packets. The maximum hop count of BPDUs affects the BPDU lifetime, and thus affects the network topology.

In an MST region, the BPDU hop count decreases by 1 each time the BPDU passes through one device from the region root until the remaining hop count is 0, indicating that the BPDU times out. Devices discard received BPDUs with the hop count of 0.

The maximum hop count of BPDUs is 20 by default. The value does not need to be changed for a network with the scale less than 20 hops, but needs to be changed to match the actual network situation when the network scale is greater than 20 hops. Changing the maximum hop count will affect all instances.

1.8.2 Restrictions and Guidelines

Hop-count:-count: Indicates the number of devices that a BPDU can pass through before it is discarded. The value range is from 1 to 40 and the default value is **20**.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum hop count for BPDUs.

spanning-tree max-hops *hop-count*

The maximum hop count of BPDUs is 20 by default.

1.9 Configuring Fast Convergence of Spanning Trees

1.9.1 Overview

In a full-duplex point-to-point link, an interface supporting RSTP first enters discarding state after port role election is complete, and then performs a Proposal/Agreement handshake with the connected bridge to quickly enter forwarding state.

Only ports in point-to-point connection state support fast convergence. Ports in shared connection state do not support fast convergence. See Fast Convergence of RSTP.

1.9.2 Restrictions and Guidelines

- If the connection type is not configured, the device automatically sets the connection type of an interface based on the duplex state of the interface. When an interface works in full-duplex mode, the connection type of the interface is point-to-point. When an interface works in half-duplex mode, the connection type of the interface is shared (non point-to-point).
- You can forcibly configure the interface connection type. The parameter **point-to-point** indicates the point-to-point connection type and **shared** indicates the shared connection type.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure fast convergence for spanning trees.

spanning-tree link-type { **point-to-point** | **shared** }

The default connection type of an interface is auto mode. If an interface works in full-duplex mode, the connection type is point-to-point. If an interface works in half-duplex mode, the connection type is shared.

1.10 Enabling Protocol Migration

1.10.1 Overview

1. Compatibility of Different Protocols

If a device running STP receives an RST BPDU or MST BPDU, it ignores or discards the BPDU, resulting in incompatibility between the device running STP and other devices running RSTP or MSTP.

However, a device running RSTP or MSTP can recognize and process STP protocol packets from other devices. RSTP and MSTP are capable of automatically determining the protocol type supported by the connected bridge based on the version of received BPDUs. If the peer supports STP, after port role election is complete, RSTP and MSTP wait for twice the period of **Forward Delay** (30s by default) before entering forwarding state according to the STP status transition mechanism.

RSTP can process the CIST part of MST BPDUs. Therefore, MSTP does not have to send RST BPDUs to ensure RSTP compatibility.

Each device running STP or RSTP is a separate region, and does not belong to the same region with any other devices.

2. Protocol Migration Principle

When both RSTP and STP are used, a problem shown in Figure 1-16 may occur: Device A supports RSTP, Device B supports only STP, and the two devices are connected to each other. Device A judges that the peer device supports only STP, and sends STP BPDUs to ensure compatibility with the peer device. After Device B is replaced with Device C supporting RSTP, Device A still runs STP and sends STP BPDUs to the peer device. In this case, Device C mistakenly judges that Device A supports only STP. Finally, both devices run STP and the spanning tree convergence speed is greatly reduced. Hence, the protocol migration function emerges.

The protocol migration function enabled on Device C clears the original protocol and forces Device C to send RST BPDUs. Device A switches to the RSTP mode when finding that the connected bridge supports RSTP. Then, the two devices run RSTP.

When finding that the peer device supports RSTP, the administrator can enable the protocol migration function to force the local device to send RST BPDUs to achieve protocol migration of the local and peer devices.

Figure 1-16 Forcing Protocol Migration to RSTP

1.10.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Clear the original protocol and force the device to migrate to the RSTP protocol.

clear spanning-tree detected-protocols [**interface** *interface-type interface-number*]

1.11 Configuring Spanning Tree Compatibility for Interfaces

1.11.1 Overview

After the spanning tree compatibility function is enabled on an interface, STP calculates whether the interface participates in the calculation of a specified instance based on the VLAN, to which the interface belongs, and the mapping between the VLAN and the instance. When the interface sends a BPDU, only the MSTI configuration message of the instance calculated by the interface, is carried to ensure compatibility with other devices.

For example, instances 1 and 2 exist on a device. Port GigabitEthernet 0/1 belongs only to VLAN 10, and VLAN 10 belongs to instance 1. If the spanning tree compatibility mode is enabled on port GigabitEthernet 0/1, the BPDU sent by port GigabitEthernet 0/1 carries only information of instance 0 (the port participates in calculation of this instance by default) and instance 1, with no information of instance 2.

1.11.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure spanning tree compatibility for an interface.

spanning-tree compatible enable

The spanning tree compatibility function of interfaces is disabled by default.

1.12 Enabling the STP Function

1.12.1 Overview

Unless otherwise specified, STP should be enabled on each device.

1.12.2 Restrictions and Guidelines

STP and the Transparent Interconnection of Lots of Links (TRILL) protocol of data centers are mutually exclusive.

1.12.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the STP function.

spanning-tree

The STP function is disabled by default.

1.13 Configuring Port Protection

1.13.1 Overview

A root bridge may receive a configuration BPDU with a higher priority due to a misconfiguration or a malicious attack using illegitimate packets in the network, and lose the current root bridge role. This can cause an incorrect network topology change. To prevent this situation, you can configure the root guard function on designated ports of the root bridge.

If the root port, master port, and alternate port on a non-root bridge periodically receive BPDUs with a higher priority from the upstream bridge, the spanning tree topology will keep unchanged. If they fail to receive high-priority BPDUs from the upstream bridge, they judge that the upstream device is faulty. Then, the bridge considers itself as the root and sets all ports as designated ports, which cause loops. To prevent this situation, you can configure the loop guard function on the above ports to enhance the device stability.

1.13.2 Restrictions and Guidelines

Root guard and loop guard cannot take effect on a port at the same time.

1.13.3 Configuration Tasks

The configuration includes the following tasks: The configuration steps below are mutually exclusive. Select one of them for configuration.

- Configuring Root Guard
- Configuring Loop Guard

1.13.4 Configuring Root Guard

1. Overview

In the network design, the root bridge and backup root bridge are usually classified into the same region. Designated ports on a root bridge may receive configuration BPDUs with a higher priority due to a misconfiguration or a malicious attack, and the root bridge loses the current root bridge role. As a result, incorrect network topology change is incurred. To prevent this situation, you can configure the root guard function on designated ports of the root bridge.

After the root guard function is enabled, the device interfaces are designated ports in all instances. If a port receives a high-priority BPDU, the port enters blocking state due to root-inconsistent. If the port fails to receive a high-priority BPDU within a period of time, it returns to the normal state.

When a port enters blocking state due to root guard, you can manually restore the port to the normal state by using two methods:

- Run the **no spanning-tree guard root** command to disable the root guard function on the port.
- Run the **spanning-tree guard none** command to disable the guard function on the port.

Caution

- When the root guard function is configured on a non-designated port, the function forcibly sets the non-designated port as a designated port. The port will inevitably receive a high-priority BPDU according

to the network design, and the port will enter blocking state due to root-inconsistent. Therefore, configuring root guard on a non-designated port can cause a communication failure.

- If a port receives a BPDU with a higher priority in an instance, it enters blocking state in this instance. If a port receives a BPDU with a higher priority in instance **0**, the port enters blocking state in all instances.

2. Restrictions and Guidelines

- In interface configuration mode, run the **spanning-tree guard root** command to enable the root guard function on an interface, or run the **no spanning-tree guard root** command to disable the root guard function of the interface.
- When a port is blocked due to root guard, you can run the **spanning-tree guard none** command in interface configuration mode to disable the root guard function and restore the port to the normal state.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

(4) Enable the root guard function.

spanning-tree guard root

The root guard function is disabled on an interface by default.

1.13.5 Configuring Loop Guard

1. Overview

The root port or alternate port of a non-root bridge may fail to receive BPDUs due to a unidirectional link failure, and the port becomes a designated port and enters forwarding state. As a result, loops occur in the network. To prevent this situation, you can configure loop guard on a non-root bridge.

After loop guard is enabled, when the root port or alternate port fails to receive BPDUs and changes to a designated port, the port will remain in discarding state until it receives a BPDU for spanning tree calculation.

Caution

- You can enable loop guard globally or on an interface.
- Before the MSTP process is restarted, a port enters the loop guard blocking state. After the MSTP process is restarted, if the port still fails to receive BPDUs, the port changes to a designated port and enters forwarding state. Therefore, you are advised to figure out the cause that a port enters the loop guard blocking state and rectify the fault before the MSTP process is restarted. Otherwise, the spanning tree topology is still abnormal after the MSTP process is restarted.

2. Restrictions and Guidelines

- In global configuration mode, run the **spanning-tree loopguard default** command to enable the loop guard

function on all interfaces, or run the **no spanning-tree loopguard default** command to disable the loop guard function of all interfaces.

- In interface configuration mode, run the **spanning-tree guard loop** command to enable the loop guard function on an interface or run the **no spanning-tree guard loop** command to disable the loop guard function of the interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the loop guard function. Select one of the following to configure.

- In global configuration mode, enable the loop guard function on all interfaces.

  spanning-tree loopguard default

  The loop guard function is disabled on an interface by default.

- In interface configuration mode, enable the loop guard function on one or a group of interfaces. Run the following commands in sequence:

  interface { *interface-type interface-number* | **range** *interface-type interface-range* }

  spanning-tree guard loop

  The loop guard function is disabled on an interface by default.

1.14 Configuring BPDU Source MAC Address Check

1.14.1 Overview

This section describes how to enable the BPDU source MAC address check function to prevent BPDU attacks. After the function is enabled on a device, the device receives only BPDU frames from specified source MAC addresses and discards other BPDU frames.

1. BPDU Source MAC Address Check

If the peer device connects to the local device in a point-to-point manner and the MAC address of the peer device is certain, the BPDU source MAC address check function can be configured on the local device. After this function is enabled, the device receives only BPDU frames matching the designated source MAC address and discards all the other BPDU frames. Therefore, when the device encounters BPDU packet attacks, illegitimate BPDU packets can be identified and discarded to prevent the MSTP function failure due to the attacks.

2. Filtering of BPDUs with Invalid Length

If the Ethernet length field in a BPDU frame exceeds 1,500, this illegitimate BPDU frame will be discarded.

1.14.2 Restrictions and Guidelines

- In interface configuration mode, run the **bpdu src-mac-check** *H.H.H* command to enable the BPDU source MAC address check function on an interface, or run the **no bpdu src-mac-check** command to disable the

BPDU source MAC address check function of the interface.

- *H.H.H* indicates that only BPDU frames with the source MAC address matching this address are received. Only one filter MAC address can be configured for one interface.
- If the configured MAC address is incorrect, required BPDU frames may be discarded.

1.14.3 Prerequisites

Configure an interface as an L2 switching port before configuring this function.

1.14.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

(4) Enable BPDU source MAC address check so that only BPDUs with the source MAC address matching *H.H.H* are received.

bpdu src-mac-check *H.H.H*

The BPDU source MAC address check function is disabled on an interface by default.

1.15 Configuring an Edge Port

1.15.1 Overview

After the spanning tree role election is complete, a designated port needs to wait for twice the period of **Forward Delay** (2 × 15 = 30s) before entering forwarding state. Designated ports can be converted into edge ports via automatic recognition or manual configuration. Edge ports can rapidly enter forwarding state without waiting for twice the period of **Forward Delay**. If an edge port receives a BPDU, it transitions from forwarding state to disabled state, changes to a non-edge port, and participates in the spanning tree calculation.

- Autoedge

  If the autoedge function is enabled on a designated port and the port fails to receive a BPDU from the downstream device within a certain period of time (3s), the port judges that the connected peer device is a network terminal. Then, the designated port changes to an edge port and rapidly enters forwarding state.

- Port fast

  If you are sure that a designated port is directly connected to a network terminal, you can manually configure port fast rather than rely on the autoedge function. A manually configured edge port rapidly enters forwarding state without waiting for twice the period of **Forward Delay**.

1.15.2 Restrictions and Guidelines

When autoedge conflicts with the edge port manually configured via port fast, the manual configuration prevails.

Unless otherwise specified, do not disable the autoedge function.

1.15.3 Configuration Tasks

The configuration includes the following tasks:

- Configuring Autoedge
- Configuring the Port Fast Attribute

1.15.4 Configuring Autoedge

1. Overview

After the spanning tree role election is complete, a designated port needs to wait for twice the period of **Forward Delay** (2 × 15 = 30s) before entering forwarding state. If the autoedge function is enabled on a designated port and the port fails to receive a BPDU from the downstream device within a certain period of time (3s), the port judges that the connected peer device is a network terminal. Then, the designated port changes to an edge port and directly enters forwarding state. If an edge port receives a BPDU, it transitions from forwarding state to disabled state, changes to a non-edge port, and participates in the spanning tree calculation.

Caution

- STP does not support this function.
- This function applies only to designated ports, and takes effect only in the process of fast negotiation between a designated port and a downstream port and the designated port has not entered forwarding state in this process. If a designated port has been in forwarding state, the autoedge function does not take effect. For example, if the BPDU filter function is enabled on a port and the port has transitioned to forwarding state, the autoedge function does not take effect. It takes effect only when the designated port restarts fast negotiation (for example, the network cable is removed and then inserted).

2. Restrictions and Guidelines

The **disabled** parameter is used to disable the autoedge function.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the autoedge function.

spanning-tree autoedge [**disabled**]

The autoedge function is enabled by default.

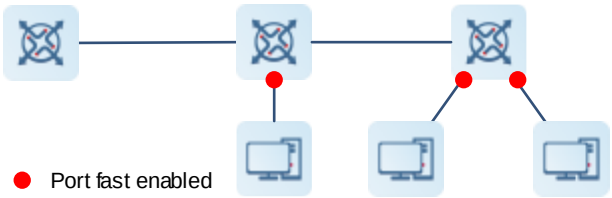
1.15.5 Configuring the Port Fast Attribute

1. Overview

After the spanning tree role election is complete, a designated port needs to wait for twice the period of **Forward Delay** (2 × 15 = 30s) before entering forwarding state. The autoedge function is enabled on a

designated port by default. If the port fails to receive a BPDU from the downstream device within a period of time (3s), it is automatically recognized as an edge port. If a designated port fails to receive a BPDU within the timeout time due to poor network condition, packet loss, or packet transmission/receiving delay, the device mistakenly judges that the designated port connects to a network terminal and automatically identifies the designated port as an edge port. In this network condition, you are advised to disable the autoedge function, and manually configure the interface connected to a terminal as an edge port according to the network plan. When you are sure that a designated port is directly connected to a network terminal, configure the port fast attribute manually rather than rely on the autoedge function. A manually configured edge port enters forwarding state without waiting for twice the period of **Forward Delay**. If an edge port receives a BPDU, it transitions from forwarding state to disabled state, changes to a non-edge port, and participates in the spanning tree calculation.

Figure 1-17 Positions of Edge Ports



2. Restrictions and Guidelines

- In global configuration mode, run the **no spanning-tree portfast default** command to restore an interface to a non-edge port.
- In interface configuration mode, run the **spanning-tree portfast disabled** command to configure an interface as a non-edge port.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an interface as an edge port. Select one of the following to configure.

- In global configuration mode, configure all interfaces as edge ports.

  spanning-tree portfast default

  Interfaces are non-edge ports by default.

- In interface configuration mode, configure a designated port as an edge port. Run the following commands in sequence:

  interface { *interface-type interface-number* | **range** *interface-type interface-range* }

  spanning-tree portfast

  Interfaces are non-edge ports by default.

1.16 Configuring BPDU Guard or BPDU Filter

1.16.1 Overview

If a device interface is directly connected to a network terminal, BPDU guard or BPDU filter can be configured on the interface to prevent illegitimate access, BPDU attacks, or loops in downstream devices. BPDU guard and BPDU filter can be enabled globally and take effect only on edge ports, or enabled and take effect only on specific interfaces.

1.16.2 Restrictions and Guidelines

BPDU filter has a higher priority than BPDU guard. If both BPDU filter and BPDU guard are enabled on an interface, only BPDU filter takes effect.

1.16.3 Configuration Tasks

The configuration includes the following tasks:

- Configuring BPDU Guard
- Configuring BPDU Filter

1.16.4 Configuring BPDU Guard

1. Overview

Edge ports do not receive BPDUs in normal cases. If an edge port is attacked by forged BPDUs or an illegitimate device is added to the network, the edge port will receive BPDUs, change to a non-edge port, and participate in spanning tree calculation, resulting in network flapping.

The BPDU guard function aims to defend against BPDU packet attacks and illegitimate access. If this function is enabled, a port enters the error-disabled state when receiving a BPDU, indicating that a port exception occurs. Then, the device disables the port, which can be restored to the normal state only through the errdisable recovery function.

BPDU guard can be enabled globally or on specific interfaces. The global BPDU guard function takes effect only on edge ports. The BPDU guard function takes effect on interfaces regardless of whether the interfaces are edge ports.

2. Restrictions and Guidelines

- In the global BPDU guard configuration command, the **no** parameter is used to disable the global BPDU guard function.
- In the interface BPDU guard configuration command, the **disabled** parameter is used to disable the BPDU guard function on a specific interface.
- A port in error-disabled state can be restored automatically or manually. The **errdisable recovery** [**interval** *seconds*] command is used to configure the auto-recovery interval, in seconds. The value range is from 30 to 86400. The errdisable recovery function is disabled on a port by default and no default recovery interval is available. To restore a port in error-disabled state manually, run the **errdisable recovery** command. See *Configuring Ethernet Interface*.
- Run the **show spanning-tree** command to display the configuration.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the BPDU guard function. Select one of the following to configure.

- Enable the global BPDU guard function. The function takes effect only on edge ports.

  spanning-tree portfast bpduguard default

  The global BPDU guard function is disabled by default.

- Enable the BPDU guard function. Run the following commands in sequence:

  interface { *interface-type interface-number* | **range** *interface-type interface-range* }

  spanning-tree bpduguard enabled

  The BPDU guard function is disabled by default.

1.16.5 Configuring BPDU Filter

1. Overview

BPDU filter is a method of preventing BPDU attacks. When BPDU filter is enabled, a port neither sends nor receives BPDUs, but directly enters forwarding state. If a port receives a BPDU, it transitions from forwarding state to disabled state, the BPDU filter function automatically fails, and the port participates in spanning tree calculation.

BPDU filter can be enabled globally or on specific interfaces. The global BPDU filter function takes effect only on edge ports. The BPDU guard function takes effect on interfaces regardless of whether the interfaces are edge ports.

2. Restrictions and Guidelines

- In the global BPDU filter configuration command, the **no** parameter is used to disable the global BPDU filter function.
- In the interface BPDU filter configuration command, the **enabled** parameter is used to enable the BPDU filter function and the **disabled** parameter is used to disable the BPDU filter function.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the BPDU filter function. Select one of the following to configure.

- Enable the global BPDU filter function. The function takes effect only on edge ports.

  spanning-tree portfast bpdufilter default

  The global BPDU filter function is disabled by default.

- Enable the BPDU filter function. Run the following commands in sequence:

  interface { *interface-type interface-number* | **range** *interface-type interface-range* }

  spanning-tree bpdufilter enabled

  The BPDU filter function is disabled by default.

1.17 Configuring TC Attack Defense Functions

1.17.1 Overview

When the downstream network topology changes, a port generates a TC packet (that is, TCN BPDU; see Table 1-4 for details) to notify the upstream device of the spanning tree change. After receiving the TCN BPDU, the port copies the BPDU and forwards it to upstream devices until the root bridge receives the BPDU. This is called TC diffusion. After receiving a TC packet, a device deletes dynamic MAC addresses and ARP entries that have been learned, and an L3 device also enables the fast forwarding module to change the port status of ARP entries.

If a device is attacked by forged TC packets, it frequently performs the deletion operation, which occupies excessive device resources and makes the device overburdened. After TC packet attacks diffuse to the whole network, the performance of devices throughout the network will deteriorate and the network stability will be affected. Therefore, TC protection, TC guard, and TC filter arise to solve this problem.

- TC protection

After TC protection is enabled on a device, the device performs only one deletion operation within a period of time (generally 4s) after receiving TC packets, and monitors whether any TC packet is received in this period. If the device receives TC packets in this period, it performs another deletion operation after the period expires, to prevent frequent deletion of MAC address entries and ARP entries.

- TC guard

TC protection can reduce the frequency of deleting dynamic MAC address entries and ARP entries, but many deletion operations still need to be performed in the case of TC packet attacks, which affects the normal operation of devices. In addition, TC packets still are diffused in the network and the entire network is affected. For this, the TC guard function emerges.

After TC guard is enabled on a port, the port will not diffuse TC packets to other ports of the device that participate in spanning tree calculation, so as to effectively control possible TC attacks in the network and retain the network stability. Especially on L3 devices, this function can effectively prevent interruption of core routes caused by access device flapping.

There are two situations of no diffusion: TC packets received by a port from other ports are not diffused; TC packets generated by a port are not diffused. TC packets generated by a port refer that, when the port status changes (for example, transition from blocking state to forwarding state), the port generates TC packets, indicating that the topology may have changed.

Caution

- The TC guard function will also limit the propagation of normal TC packets. When a spanning tree network topology changes, devices cannot obtain topology change information and the topology cannot be restored, resulting in a communication interruption. Therefore, it is recommended that the TC guard function be enabled only when the network is attacked by illegitimate TC packets.

- If the global TC guard function is enabled, all ports will not diffuse TC packets. The global TC guard function is applicable to desktop access devices.
- If the interface TC guard function is enabled, the port will not diffuse TC packets. The interface TC guard function is applicable to uplink ports, especially the ports that connect aggregation devices to core devices.

- TC filter

TC guard blocks the diffusion of all TC packets, including normal TC packets generated in the case of a topology change. As a result, devices in the network cannot perceive the topology change and fail to clear MAC address entries and ARP entries of relevant ports in time, and errors occur in data forwarding. Hence, the TC filter function emerges.

TC filter refers that a port does not process TC packets received from other ports but processes TC packets generated due to the normal topology change of the port.

This function solves the problems of MAC address entry clearing and core route interruption caused by frequent up/down state switching of ports with port fast not configured. It also ensures that core routing entries are updated in time when a topology change occurs.

1.17.2 Restrictions and Guidelines

It is recommended that the TC attack defense functions be enabled only when the network is attacked by TC packets.

1.17.3 Configuration Tasks

The configuration includes the following tasks:

- Configuring TC Protection
- Configuring TC Guard
- Configuring TC Filter

1.17.4 Configuring TC Protection

1. Overview

After TC protection is enabled, the device performs only one deletion operation within a period of time (generally 4s) after receiving TC packets. This can prevent frequent deletion of MAC address entries and ARP entries.

2. Restrictions and Guidelines

TC protection can be enabled or disabled only globally and takes effect on all interfaces. Run the **spanning-tree tc-protection** command to enable TC protection or run the **no spanning-tree tc-protection** command to disable TC protection.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable TC protection on all interfaces.

spanning-tree tc-protection

TC protection is disabled by default.

1.17.5 Configuring TC Guard

1. Overview

After TC guard is enabled on a port, the port shields received TC packets and the TC packets generated by the port so that the TC packets are not diffused to other ports. In this way, possible TC attacks in the network are effectively contained, ensuring network stability.

2. Restrictions and Guidelines

- In global configuration mode, the TC guard function configuration takes effect on all interfaces. Run the **spanning-tree tc-protection tc-guard** command to enable the TC guard function or run the **no spanning-tree tc-protection tc-guard** command to disable the TC guard function.
- In interface configuration mode, the TC guard function configuration takes effect only on specific interfaces. Run the **spanning-tree tc-guard** command to enable the TC guard function or run the **no spanning-tree tc-guard** command to disable the TC guard function.
- If no TC attack exists in a network but TC guard is configured, the spread of normal TC packets is contained. When the topology changes, the device fails to clear learned MAC addresses and a packet forwarding error may occur.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the TC guard function. Select one of the following to configure.

- Enable TC guard on all interfaces.

  spanning-tree tc-protection tc-guard

  TC guard is disabled by default.

- Enable TC guard on a specific interface. Run the following commands in sequence:

  interface { *interface-type interface-number* | **range** *interface-type interface-range* }

  spanning-tree tc-guard

  TC guard is disabled by default.

1.17.6 Configuring TC Filter

1. Overview

TC filter enables a port not to process received TC packets but to process TC packets generated by the port due to topology changes.

2. Restrictions and Guidelines

TC filter can be enabled or disabled only on interfaces and takes effect on specific interfaces. In interface configuration mode, run the **spanning-tree ignore tc** command to enable the TC filter function or run the **no spanning-tree ignore tc** command to disable the TC filter function.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

(4) Enable TC filter on a specific interface.

spanning-tree ignore tc

TC filter is disabled by default.

1.18 Configuring BPDU Tunnel

1.18.1 Overview

BPDU tunnel is an L2 tunnel function based on the Layer 2 Tunnel Protocol (L2TP).

A 802.1Q (QinQ) network is usually divided into the customer network and service provider network. The basic principle of QinQ is described as follows: When a user packet is sent to a provider edge (PE), the PE considers the VLAN tag in the user packet as data, and encapsulates the VLAN tag of the service provider network into the packet so that the user packet carries two VLAN tags to traverse the service provider network. In the service provider network, the packet is forwarded based on the outer VLAN tag. When the packet leaves the service provider network, the outer VLAN tag is removed.

STP BPDUs use the BPDU dedicated address 0180.c200.0000 as the destination MAC address. Therefore, the BPDUs of the customer network and service provider network have the same destination MAC address. When a tunnel interface of a PE receives a BPDU from the customer network, the PE recognizes the BPDU as an STP packet and does not forward it because the destination MAC address of the BPDU is the BPDU dedicated address (0180.c200.0000). In addition, the PE performs spanning tree calculation based on the BPDU content, which affects the topology of the service provider network. In order to prevent the customer network BPDUs from interfering with the spanning tree calculation of the service provider network, you need to differentiate customer network BPDUs from service provider network BPDUs, that is, modify the destination MAC address in customer network BPDUs.

After the BPDU tunnel function is enabled on a tunnel interface of a PE, if the interface receives a customer network BPDU, it changes the destination MAC address in the BPDU from the BPDU dedicated address (0180.c200.0000) to the tunnel address (01d0.f800.0005 by default) and forwards the BPDU in the service provider network. When the BPDU reaches a PE at the other end, the PE restores the destination MAC address of the BPDU from the tunnel address (01d0.f800.0005 by default) to the BPDU dedicated address (0180.c200.0000) and forwards the BPDU to the peer customer network. Customer network BPDUs are transmitted through BPDU tunnels in the service provider network. In this way, the STP calculations of the

customer network and service provider network are performed separately without interfering with each other. For details, see *Configuring QinQ* and *Configuring VPDN*.

1.18.2 Restrictions and Guidelines

- This function takes effect only when it is enabled in both global configuration mode and interface configuration mode.
  - Run the **l2protocol-tunnel stp** command to enable the global BPDU tunnel function or run the **no l2protocol-tunnel stp** command to disable the global BPDU tunnel function.
  - Run the **l2protocol-tunnel stp enable** command to enable the BPDU tunnel function or run the **no l2protocol-tunnel stp enable** command to disable the BPDU tunnel function.
- Run the **l2protocol-tunnel stp tunnel-dmac** *mac-address* command to configure a BPDU tunnel address. The optional tunnel addresses of STP packets include 01d0.f800.0005 (default), 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2.

1.18.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the global BPDU tunnel function.

l2protocol-tunnel stp

The global BPDU tunnel function is disabled by default.

(4) (Optional) Configure a BPDU tunnel address.

l2protocol-tunnel stp tunnel-dmac *mac-address*

The default BPDU tunnel address is 01d0.f800.0005.

(5) Enter the interface configuration mode of the port that connects the customer network.

interface *interface-type interface-number*

(6) Enable the BPDU tunnel function on the interface.

l2protocol-tunnel stp enable

The BPDU tunnel function is disabled by default.

1.19 Configuring BPDU Transparent Transmission

1.19.1 Overview

According to the IEEE 802.1Q standard, BPDUs use 0180.c200.0000 as the destination MAC address. When a device supporting IEEE 802.1Q receives a frame with the destination address of 0180.c200.0000, it recognizes the frame as a BPDU and will not forward it.

However, in the actual network deployment, some BPDU frames need to be transparently transmitted by devices. For example, STP is disabled on Device A but enabled on Device B and Device C connected through

Device A. In this case, Device A needs to transparently transmit BPDU frames so that Device B and Device C can normally calculate and generate spanning trees.

1.19.2 Restrictions and Guidelines

- BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU frames. If STP is enabled on a service provider network device and the device is required to transmit customer network BPDUs without affecting the spanning tree of the service provider network, use the BPDU tunnel function.
- In global configuration mode, run the **bridge-frame forwarding protocol bpdu** command to enable the BPDU transparent transmission function, or run the **no bridge-frame forwarding protocol bpdu** command to disable the BPDU transparent transmission function.

1.19.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the BPDU transparent transmission function.

bridge-frame forwarding protocol bpdu

BPDU transparent transmission is disabled by default.

1.20 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** commands to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging switch immediately after use.

Run the **clear** commands to clear information.

Caution

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

Table 1-12 Monitoring

Command	Purpose
show spanning-tree [**forward-time** | **hello-time** | **max-age** | **max-hops** | **mst** *instance-id* | **pathcost method** | **tx-hold-count**]	Displays the global spanning tree configuration.
show spanning-tree counters	Displays statistics on sent and received STP packets.

Command	Purpose
show spanning-tree inconsistentports	Displays ports blocked due to root guard or loop guard.
show spanning-tree summary	Displays the spanning tree topology and port forwarding status.
show spanning-tree [**mst** *instance-id*] **interface** *interface-type interface-number* [**bpdufilter** | **bpduguard** | **link-type** | **portfast**]	Displays the spanning tree configuration and status information of an interface by interface type and number.
show spanning-tree [**mst** *instance-id*] *port-index*	Displays the spanning tree configuration and status information of an interface by interface number.
show spanning-tree mst configuration	Displays the MST region configuration.
show spanning-tree mst *instance-id* **topochange record**	Displays the topology change information of an interface in a specified instance.
show l2protocol-tunnel stp	Displays BPDU tunnel information.
debug mstp all	Debugs STP, RSTP, and MSTP.
debug mstp gr	Debugs the spanning tree GR function.
debug mstp rx	Debugs the BPDU receiving.
debug mstp tx	Debugs BPDU transmission.
debug mstp event	Debugs spanning tree events.
debug mstp loopguard	Debugs spanning tree loop guard.
debug mstp rootguard	Debugs spanning tree root guard.
debug mstp bridgedetect	Debugs the bridge detect state machine.
debug mstp portinfo	Debugs the port information state machine.
debug mstp protomigrat	Debugs the port protocol migration state machine.
debug mstp topochange	Debugs the spanning tree topology changes.
debug mstp receive	Debugs the spanning tree receiving state machine.
debug mstp roletran	Debugs the port role transition state machine.
debug mstp statetran	Debugs the port state transition state machine.
debug mstp transmit	Debugs the MSTP transmission state machine.
clear spanning-tree counters [**interface** *interface-type interface-number*]	Clears statistics on packets sent and received by a port.

Command	Purpose
clear spanning-tree mst *instance-id* **topochange record**	Clears the STP topology change information.

1.21 Configuration Examples

1.21.1 Configuring MSTP

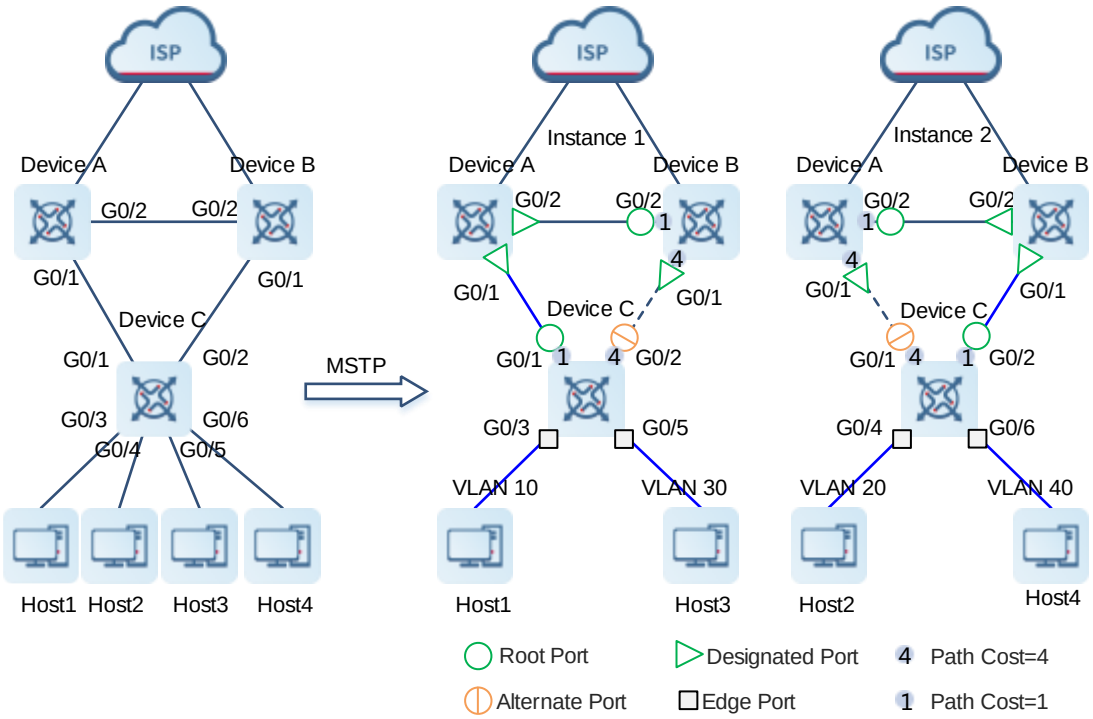
1. Requirements

The topology shown in Figure 1-18 includes two layers: Device A and Device B are in the core layer, Device C is in the access layer, and Device C connects to intranet terminals. There are four VLANs in the intranet. The configured MSTP needs to meet the following requirements:

- The spanning tree root bridge of VLAN 10 and VLAN 30 is Device A and data is forwarded through port GigabitEthernet 0/1 of Device C.
- The spanning tree root bridge of VLAN 20 and VLAN 40 is Device B and data is forwarded through port GigabitEthernet 0/2 of Device C.
- Enable loop guard on the root ports of Device C. Enable BPDU guard on the edge ports of Device C that connect to terminals.

2. Topology

Figure 1-18 MSTP Basic Topology



3. Notes

- Create the same VLANs on Devices A, B, and C and configure the same instance mappings: Map instance 1 to VLANs 10 and 30 and map instance 2 to VLANs 20 and 40. Instance 0 contains other VLANs that have not been created.
- The devices elect the device roles and port roles in the spanning tree by comparing the priority vector <**Root Identifier**, **Root Path Cost**, **Bridge ID**, **Port ID**>. Configure the bridge priorities and port path costs for instances so that the required topology is calculated. For the ease of management, configure the same spanning tree for instance 0 and instance 1.

  Instance 0 and instance 1:

  - Set the bridge priority to 4096 for Device A and 8192 for Device B, and use the default bridge priority 32768 (no configuration is required) for Device C so that Device A becomes the root bridge.
  - On Device B, set the path cost to 1 for port GigabitEthernet 0/2 and 4 for port GigabitEthernet 0/1 so that port GigabitEthernet 0/2 becomes the root port of Device B.
  - On Device C, set the path cost to 1 for port GigabitEthernet 0/1 and 4 for port GigabitEthernet 0/2 so that port GigabitEthernet 0/1 becomes the root port of Device C.
  - The bridge priority of Device B is 8192, which is higher than that of Device C (32768). Therefore, port GigabitEthernet 0/1 of Device B is elected as the designated port and port GigabitEthernet 0/2 of Device C is elected as the alternate port.

  Instance 2:

  - Set the bridge priority to 4096 for Device B and 8192 for Device A, and use the default bridge priority 32768 (no configuration is required) for Device C so that Device B becomes the root bridge.
  - On Device A, set the path cost to 1 for port GigabitEthernet 0/2 and 4 for port GigabitEthernet 0/1 so that port GigabitEthernet 0/2 becomes the root port of Device A.
  - On Device C, set the path cost to 1 for port GigabitEthernet 0/2 and 4 for port GigabitEthernet 0/1 so that port GigabitEthernet 0/2 becomes the root port of Device C.
  - The bridge priority of Device A is 8192, which is higher than that of Device C (32768). Therefore, port GigabitEthernet 0/1 of Device A is elected as the designated port and port GigabitEthernet 0/1 of Device C is elected as the alternate port.
- Configure MSTP loop guard on ports GigabitEthernet 0/1–0/2 of Device C. When the root port or backup port fails to receive BPDUs and changes to a designated port, the port will remain in discarding state until it receives BPDUs for spanning tree calculation.
- On Device C, configure ports GigabitEthernet 0/3–0/6 that connect to terminals as edge ports. The autoedge function is enabled by default. If ports GigabitEthernet 0/3–0/6 fail to receive BPDUs within 3s after being elected as designated ports, they are automatically recognized as edge ports and immediately enters forwarding state. Packet loss or packet transmission/receiving delay in the network may affect the autoedge function. Therefore, disable the autoedge function, manually configure the ports as edge ports, and enable the BPDU guard function.
- Enable the STP function globally on Devices A, B, and C and use the default MSTP mode.
- Configure interconnected ports among Devices A, and B, and C as trunk ports and configure the ports to allow all VLAN traffic to pass. Add the interfaces of Device C that connect to terminals to their respective VLANs.

4. Procedure

(1) Configure Device A.

Create VLANs and configure instance mappings.

```
DeviceA>enable
DeviceA# configure terminal
DeviceA(config)# vlan range 10,20,30,40
DeviceA(config-vlan-range)# exit
DeviceA(config)# spanning-tree mst configuration
DeviceA(config-mst)# instance 1 vlan 10,30
DeviceA(config-mst)# instance 2 vlan 20,40
```

Set the bridge priority to 4094 for instances 0 and 1 and 8192 for instance 2.

```
DeviceA(config-mst)# spanning-tree mst 0 priority 4096
DeviceA(config)# spanning-tree mst configuration
DeviceA(config-mst)# spanning-tree mst 1 priority 4096
DeviceA(config)# spanning-tree mst configuration
DeviceA(config-mst)# spanning-tree mst 2 priority 8192
```

Configure port GigabitEthernet 0/2 as a trunk port. In instance 2, set the path cost of the port to 1.

```
DeviceA(config)# interface range gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# switchport
DeviceA(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/2)# spanning-tree mst 2 cost 1
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

Configure port GigabitEthernet 0/1 as a trunk port. In instance 2, set the path cost of the port to 4.

```
DeviceA(config)# interface range gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/1)# spanning-tree mst 2 cost 4
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Enable the STP function globally.

```
DeviceA(config)# spanning-tree
DeviceA(config)# end
DeviceA# write
```

(2) Configure Device B.

Create VLANs and configure instance mappings.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan range 10,20,30,40
DeviceB(config-vlan-range)# exit
DeviceB(config)# spanning-tree mst configuration
DeviceB(config-mst)# instance 1 vlan 10,30
DeviceB(config-mst)# instance 2 vlan 20,40
```

Set the bridge priority to 4094 for instance 2 and 8192 for instance 0 and instance 1.

```
DeviceB(config-mst)# spanning-tree mst 0 priority 8192
DeviceB(config)# spanning-tree mst configuration
DeviceB(config-mst)# spanning-tree mst 1 priority 8192
DeviceB(config)# spanning-tree mst configuration
DeviceB(config-mst)# spanning-tree mst 2 priority 4096
```

Configure port GigabitEthernet 0/2 as a trunk port. In instances 0 and 1, set the path cost of the port to 1.

```
DeviceB(config)# interface range gigabitethernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# switchport
DeviceB(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/2)# spanning-tree mst 0 cost 1
DeviceB(config-if-GigabitEthernet 0/2)# spanning-tree mst 1 cost 1
DeviceB(config-if-GigabitEthernet 0/2)# exit
```

Configure port GigabitEthernet 0/1 as a trunk port. In instances 0 and 1, set the path cost of the port to 4.

```
DeviceB(config)# interface range gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# switchport
DeviceB(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/1)# spanning-tree mst 0 cost 4
DeviceB(config-if-GigabitEthernet 0/1)# spanning-tree mst 1 cost 4
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Enable the STP function globally.

```
DeviceB(config)# spanning-tree
DeviceB(config)# end
DeviceB# write
```

(3) Configure Device C.

Create VLANs and configure instance mappings.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# vlan range 10,20,30,40
DeviceC(config-vlan-range)# exit
DeviceC(config)# spanning-tree mst configuration
DeviceC(config-mst)# instance 1 vlan 10,30
DeviceC(config-mst)# instance 2 vlan 20,40
DeviceC(config-mst)# exit
```

Configure uplink port GigabitEthernet 0/1 as a trunk port. In instances 0 and 1, set the path cost of the port to 1. In instance 2, set the path cost of the port to 4. Configure loop guard on the uplink port.

```
DeviceC(config)# interface gigabitethernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# switchport
DeviceC(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceC(config-if-GigabitEthernet 0/1)# spanning-tree mst 0 cost 1
DeviceC(config-if-GigabitEthernet 0/1)# spanning-tree mst 1 cost 1
DeviceC(config-if-GigabitEthernet 0/1)# spanning-tree mst 2 cost 4
DeviceC(config-if-GigabitEthernet 0/1)# spanning-tree guard loop
DeviceC(config-if-GigabitEthernet 0/1)# exit
```

Configure uplink port GigabitEthernet 0/2 as a trunk port. In instance 2, set the path cost of the port to 1. In instances 0 and 1, set the port path cost to 4. Configure loop guard on the uplink port.

```
DeviceC(config)# interface gigabitethernet 0/2
DeviceC(config-if-GigabitEthernet 0/2)# switchport
DeviceC(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceC(config-if-GigabitEthernet 0/2)# spanning-tree mst 0 cost 4
DeviceC(config-if-GigabitEthernet 0/2)# spanning-tree mst 1 cost 4
DeviceC(config-if-GigabitEthernet 0/2)# spanning-tree mst 2 cost 1
DeviceC(config-if-GigabitEthernet 0/2)# spanning-tree guard loop
DeviceC(config-if-GigabitEthernet 0/2)# exit
```

Add downlink ports GigabitEthernet 0/3–0/6 to VLANs. Configure the ports as edge ports and configure BPDU guard.

```
DeviceC(config)# interface gigabitethernet 0/3
DeviceC(config-if-GigabitEthernet 0/3)# switchport
DeviceC(config-if-GigabitEthernet 0/3)# switchport mode access
DeviceC(config-if-GigabitEthernet 0/3)# switchport access vlan 10
DeviceC(config-if-GigabitEthernet 0/3)# spanning-tree autoedge disabled
DeviceC(config-if-GigabitEthernet 0/3)# spanning-tree portfast
DeviceC(config-if-GigabitEthernet 0/3)# spanning-tree bpduguard enable
DeviceC(config-if-GigabitEthernet 0/3)# exit
DeviceC(config)# interface gigabitethernet 0/4
DeviceC(config-if-GigabitEthernet 0/4)# switchport
DeviceC(config-if-GigabitEthernet 0/4)# switchport mode access
DeviceC(config-if-GigabitEthernet 0/4)# switchport access vlan 20
DeviceC(config-if-GigabitEthernet 0/4)# spanning-tree autoedge disabled
DeviceC(config-if-GigabitEthernet 0/4)# spanning-tree portfast
DeviceC(config-if-GigabitEthernet 0/4)# spanning-tree bpduguard enable
DeviceC(config-if-GigabitEthernet 0/4)# exit
DeviceC(config)# interface gigabitethernet 0/5
DeviceC(config-if-GigabitEthernet 0/5)# switchport
DeviceC(config-if-GigabitEthernet 0/5)# switchport mode access
DeviceC(config-if-GigabitEthernet 0/5)# switchport access vlan 30
DeviceC(config-if-GigabitEthernet 0/5)# spanning-tree autoedge disabled
DeviceC(config-if-GigabitEthernet 0/5)# spanning-tree portfast
DeviceC(config-if-GigabitEthernet 0/5)# spanning-tree bpduguard enable
DeviceC(config-if-GigabitEthernet 0/5)# exit
DeviceC(config)# interface gigabitethernet 0/6
DeviceC(config-if-GigabitEthernet 0/6)# switchport
DeviceC(config-if-GigabitEthernet 0/6)# switchport mode access
DeviceC(config-if-GigabitEthernet 0/6)# switchport access vlan 40
DeviceC(config-if-GigabitEthernet 0/6)# spanning-tree autoedge disabled
DeviceC(config-if-GigabitEthernet 0/6)# spanning-tree portfast
DeviceC(config-if-GigabitEthernet 0/6)# spanning-tree bpduguard enable
DeviceC(config-if-GigabitEthernet 0/6)# exit
```

Enable the STP function globally.

```
DeviceC(config)# spanning-tree
DeviceC(config)# end
DeviceC# write
```

5. Verification

(1) Verify that instance mappings on the devices are the same.

Check instance mappings on Device A.

```
DeviceA# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    :
Revision : 0
Instance  Vlans Mapped
-------- -------------------------------------------
0       : 1-9, 11-19, 21-29, 31-39, 41-4094
1       : 10, 30
2       : 20, 40
---------------------------------------------------
```

Check instance mappings on Device B.

```
DeviceB# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    :
Revision : 0
Instance  Vlans Mapped
-------- -------------------------------------------
0       : 1-9, 11-19, 21-29, 31-39, 41-4094
1       : 10, 30
2       : 20, 40
---------------------------------------------------
```

Check instance mappings on Device C.

```
DeviceC# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    :
Revision : 0
Instance  Vlans Mapped
-------- -------------------------------------------
0       : 1-9, 11-19, 21-29, 31-39, 41-4094
1       : 10, 30
2       : 20, 40
---------------------------------------------------
```

(2) Check the instance spanning tree topology and port forwarding status on Device A.

In instances 0 and 1, Device A (0074.9cee.f49e) is the root bridge. Ports GigabitEthernet 0/1–0/2 of Device A are designated ports. They are all in forwarding state.

```
DeviceA# show spanning-tree summary
Spanning tree enabled protocol mstp
```

```
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID    Priority    4096
           Address     0074.9cee.f49e
           this bridge is root
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    4096
           Address     0074.9cee.f49e
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Desg FWD 200000    128     False    P2p
Gi0/2           Desg FWD 20000     128     False    P2p

MST 1 vlans map : 10, 30
  Region Root Priority   4096
           Address     0074.9cee.f49e
           this bridge is region root

  Bridge ID  Priority    4096
           Address     0074.9cee.f49e

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Desg FWD 200000    128     False    P2p
Gi0/2           Desg FWD 20000     128     False    P2p
```

In instance 2, Device B (00d0.f8ee.8c1e) is the root bridge. Port GigabitEthernet 0/2 of Device A is the root port and the port path cost is 1. Port GigabitEthernet 0/1 of Device A is the designated port and the port path cost is 4. The two ports are in forwarding state.

```
MST 2 vlans map : 20, 40
  Region Root Priority   4096
           Address     00d0.f8ee.8c1e
           this bridge is region root

  Bridge ID  Priority    8192
           Address     0074.9cee.f49e

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Desg FWD 4         128     False    P2p
Gi0/2           Root FWD 1         128     False    P2p
```

(3) Check the instance spanning tree topology and port forwarding status on Device B.

In instances 0 and 1, Device A (0074.9cee.f49e) is the root bridge. Port GigabitEthernet 0/1 of Device B is the root port and the port path cost is 1. Port GigabitEthernet 0/2 of Device B is the designated port and the port path cost is 4. The two ports are in forwarding state.

```
DeviceB# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID    Priority    4096
           Address     0074.9cee.f49e
           this bridge is root
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    8192
           Address     00d0.f8ee.8c1e
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Root FWD 1         128     False    P2p
Gi0/2           Desg FWD 4         128     False    P2p

MST 1 vlans map : 10, 30
  Region Root Priority   4096
           Address     0074.9cee.f49e
           this bridge is region root

  Bridge ID  Priority    8192
           Address     00d0.f8ee.8c1e

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Root FWD 1         128     False    P2p
Gi0/2           Desg FWD 4         128     False    P2p
```

In instance 2, Device B (00d0.f8ee.8c1e) is the root bridge. Ports GigabitEthernet 0/1–0/2 of Device B are designated ports. They are all in forwarding state.

```
MST 2 vlans map : 20, 40
  Region Root Priority   4096
           Address     00d0.f8ee.8c1e
           this bridge is region root

  Bridge ID  Priority    4096
           Address     00d0.f8ee.8c1e

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Desg FWD 20000     128     False    P2p
```

```
Gi0/2          Desg FWD 20000     128     False    P2p
```

(4) Check the instance spanning tree topology and port forwarding status on Device C.

In instances 0 and 1, Device A (0074.9cee.f49e) is the root bridge. Port GigabitEthernet 0/1 of Device C is the root port and the port path cost is 1. The port is in forwarding state. Port GigabitEthernet 0/2 of Device C is the alternate port and the port path cost is 4. The port is in blocking state. Ports GigabitEthernet 0/3–0/6 of Device C are edge ports. They are all in forwarding state.

```
DeviceC# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID    Priority    4096
           Address     0074.9cee.f49e
           this bridge is root
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
           Address     0074.9cee.53ca
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1          Root FWD 1         128     False    P2p
Gi0/2          Altn BLK 4         128     False    P2p
Gi0/3          Desg FWD 20000     128     True     P2p
Gi0/4          Desg FWD 20000     128     True     P2p
Gi0/5          Desg FWD 20000     128     True     P2p
Gi0/6          Desg FWD 20000     128     True     P2p

MST 1 vlans map : 10, 30
  Region Root Priority   4096
           Address     0074.9cee.f49e
           this bridge is region root

  Bridge ID  Priority    32768
           Address     0074.9cee.53ca

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1          Root FWD 1         128     False    P2p
Gi0/2          Altn BLK 4         128     False    P2p
Gi0/3          Desg FWD 20000     128     True     P2p
Gi0/4          Desg FWD 20000     128     True     P2p
Gi0/5          Desg FWD 20000     128     True     P2p
Gi0/6          Desg FWD 20000     128     True     P2p
```

In instance 2, Device B (00d0.f8ee.8c1e) is the root bridge. Port GigabitEthernet 0/2 of Device C is the root port and the port path cost is 1. The port is in forwarding state. Port GigabitEthernet 0/1 of Device C is the

alternate port and the port path cost is 4. The port is in blocking state. Ports GigabitEthernet 0/3–0/6 of Device C are edge ports. They are all in forwarding state.

```
MST 2 vlans map : 20, 40
  Region Root Priority   4096
           Address    00d0.f8ee.8c1e
           this bridge is region root

  Bridge ID  Priority   32768
           Address    0074.9cee.53ca

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Altn BLK 4         128     False    P2p
Gi0/2           Root FWD 1         128     False    P2p
Gi0/3           Desg FWD 20000     128     True     P2p
Gi0/4           Desg FWD 20000     128     True     P2p
Gi0/5           Desg FWD 20000     128     True     P2p
Gi0/6           Desg FWD 20000     128     True     P2p
```

(5) Check "DesignatedRoot", "RootPort", and "RootCost" of each device in instance 1. Check the "DesignatedRoot", "RootPort", and "RootCost" of each device in instances 0 and 2.

Device A is the root and the root path cost is 0.

```
DeviceA# show spanning-tree mst 1
###### MST 1 vlans mapped : 10, 30
BridgeAddr : 0074.9cee.f49e
Priority: 4096
TimeSinceTopologyChange : 0d:0h:16m:29s
TopologyChanges : 7
DesignatedRoot : 4097.0074.9cee.f49e
RootCost : 0
RootPort : 0
```

The root path cost from Device B to the root (4097.0074.9cee.f49e) through root port GigabitEthernet 0/2 is 1.

```
DeviceB# show spanning-tree mst 1
###### MST 1 vlans mapped : 10, 30
BridgeAddr : 00d0.f8ee.8c1e
Priority: 8192
TimeSinceTopologyChange : 0d:0h:16m:27s
TopologyChanges : 7
DesignatedRoot : 4097.0074.9cee.f49e
RootCost : 1
RootPort : GigabitEthernet 0/2
```

The root path cost from Device C to the root (4097.0074.9cee.f49e) through root port GigabitEthernet 0/1 is 1.

```
DeviceC# show spanning-tree mst 1
```

```
###### MST 1 vlans mapped : 10, 30
BridgeAddr : 0074.9cee.53ca
Priority: 32768
TimeSinceTopologyChange : 0d:0h:19m:48s
TopologyChanges : 5
DesignatedRoot : 4097.0074.9cee.f49e
RootCost : 1
RootPort : GigabitEthernet 0/1
```

(6) Verify that the loop guard function ("PortGuardmode:Guard loop") on uplink ports GigabitEthernet 0/1–0/2 of Device C is enabled. The following uses GigabitEthernet 0/1 as an example.

```
DeviceC# show spanning-tree interface gigabitethernet 0/1
PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode  : Guard loop

###### MST 0 vlans mapped :1-9, 11-19, 21-29, 31-39, 41-4094
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 4096.0074.9cee.f49e
PortDesignatedCost : 0
PortDesignatedBridge :4096.0074.9cee.f49e
PortDesignatedPortPriority : 128
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost : 1
PortOperPathCost : 1
Inconsistent states : normal
PortRole : rootPort

###### MST 1 vlans mapped :10, 30
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 4097.0074.9cee.f49e
PortDesignatedCost : 0
PortDesignatedBridge :4097.0074.9cee.f49e
PortDesignatedPortPriority : 128
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost : 1
PortOperPathCost : 1
```

```
Inconsistent states : normal
PortRole : rootPort

###### MST 2 vlans mapped :20, 40
PortState : discarding
PortPriority : 128
PortDesignatedRoot : 4098.00d0.f8ee.8c1e
PortDesignatedCost : 0
PortDesignatedBridge :8194.0074.9cee.f49e
PortDesignatedPortPriority : 128
PortDesignatedPort : 1
PortForwardTransitions : 3
PortAdminPathCost : 4
PortOperPathCost : 4
Inconsistent states : normal
PortRole : alternatePort
```

(7) Verify that port fast is configured on ports GigabitEthernet 0/3–0/6 of Device C ("PortAdminPortFast : Enabled"), the ports work in port fast state ("PortOperPortFast : Enabled"), and BPDU guard is enabled on the ports (“PortBPDUGuard: Enabled”). The following uses port GigabitEthernet 0/3 as an example.

```
DeviceC# show spanning-tree interface gigabitethernet 0/3

PortAdminPortFast : Enabled
PortOperPortFast : Enabled
PortAdminAutoEdge : Disabled
PortOperAutoEdge : Enabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Enabled
PortBPDUFilter : Disabled
PortGuardmode  : None

###### MST 0 vlans mapped :1-9, 11-19, 21-29, 31-39, 41-4094
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 4096.0074.9cee.f49e
PortDesignatedCost : 0
PortDesignatedBridge :32768.0074.9cee.53ca
PortDesignatedPortPriority : 128
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : designatedPort

###### MST 1 vlans mapped :10, 30
```

```
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 4097.0074.9cee.f49e
PortDesignatedCost : 0
PortDesignatedBridge :32769.0074.9cee.53ca
PortDesignatedPortPriority : 128
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : designatedPort

###### MST 2 vlans mapped :20, 40
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 4098.00d0.f8ee.8c1e
PortDesignatedCost : 0
PortDesignatedBridge :32770.0074.9cee.53ca
PortDesignatedPortPriority : 128
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : designatedPort
```

6. Configuration Files

- Device A configuration file

```
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 30
 instance 2 vlan 20, 40
!
spanning-tree mst 0 priority 4096
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
spanning-tree
!
sysmac 0074.9cee.f49e
!
vlan range 1,10,20,30,40
!
interface GigabitEthernet 0/1
 switchport mode trunk
 spanning-tree mst 2 cost 4
```

```
!
interface GigabitEthernet 0/2
 switchport mode trunk
 spanning-tree mst 2 cost 1
```

- Device B configuration file

```
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 30
 instance 2 vlan 20, 40
!
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
spanning-tree
!
sysmac 00d0.f8ee.8c1e
!
vlan range 1,10,20,30,40
!
interface GigabitEthernet 0/1
 switchport mode trunk
 spanning-tree mst 1 cost 4
 spanning-tree mst 0 cost 4
!
interface GigabitEthernet 0/2
 switchport mode trunk
 spanning-tree mst 1 cost 1
 spanning-tree mst 0 cost 1
```

- Device C configuration file

```
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 30
 instance 2 vlan 20, 40
!
spanning-tree
!
sysmac 0074.9cee.53ca
!
vlan range 1,10,20,30,40
!
interface GigabitEthernet 0/1
 switchport mode trunk
 spanning-tree guard loop
 spanning-tree mst 2 cost 4
 spanning-tree mst 1 cost 1
```

```
 spanning-tree mst 0 cost 1
!
interface GigabitEthernet 0/2
 switchport mode trunk
 spanning-tree guard loop
 spanning-tree mst 2 cost 1
 spanning-tree mst 1 cost 4
 spanning-tree mst 0 cost 4
!
interface GigabitEthernet 0/3
 switchport access vlan 10
 spanning-tree bpduguard enable
 spanning-tree portfast
 spanning-tree autoedge disabled
!
interface GigabitEthernet 0/4
 switchport access vlan 20
 spanning-tree bpduguard enable
 spanning-tree portfast
 spanning-tree autoedge disabled
!
interface GigabitEthernet 0/5
 switchport access vlan 30
 spanning-tree bpduguard enable
 spanning-tree portfast
 spanning-tree autoedge disabled
!
interface GigabitEthernet 0/6
 switchport access vlan 40
 spanning-tree bpduguard enable
 spanning-tree portfast
 spanning-tree autoedge disabled
```

7. Common Errors

- When no bridge priority lower than that of the root bridge but higher than that of access devices is configured for non-root devices, the non-root core devices and access devices will determine upstream devices by comparing MAC addresses in the spanning tree calculation. As a result, the calculation result may not meet networking requirements.
- When no port path cost is configured for non-root devices, the spanning tree calculation result may not meet networking requirements due to different link conditions.
- The root guard function is configured on a root port, master port, or alternate port, and ports may be blocked incorrectly.

1.21.2 Configuring MSTP+VRRP

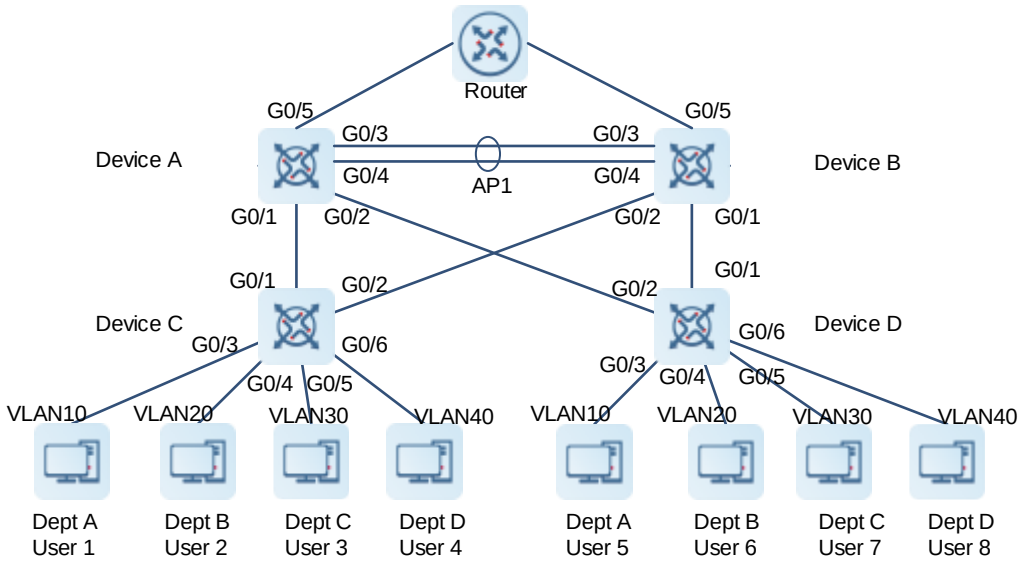
1. Requirements

The MSTP+VRRP dual-core solution is a typical application of MSTP. This solution uses a hierarchical network architecture and MSTP and Virtual Router Redundancy Protocol (VRRP) to implement redundant backup and VLAN load balancing, to enhance the network system availability. The highlight of this architecture is the hierarchical network structure. The capacity indicators, characteristics, and functions of network devices in each layer can be optimized based on their network locations and functions to boost the system stability and availability. This solution usually uses a three-layer (core layer, aggregation layer, and access layer) or two-layer (core layer and access layer) architecture. The topology shown in Figure 1-19 adopts a two-layer architecture. The networking requirements are as follows:

- Core layer: Configure multiple MSTP instances to achieve load balancing. Create instance 1 and instance 2. Map instance 1 to VLAN 10 and VLAN 30 and instance 2 to VLAN 20 and VLAN 40. Device A is the root bridge of instances 0 and instance 1 (instance 0 exists by default) as well as the VRRP master device of VLAN 10 and VLAN 30. Device B is the root bridge of instance 2 as well as the VRRP master device of VLANs 20 and 40.
- Access layer: Configure ports that are directly connected to terminals (such as PCs or servers) as edge ports and enable BPDU guard to prevent the access of unauthorized user devices.

2. Topology

Figure 1-19 MSTP+VRRP Dual-Core Topology



3. Notes

- Configure MSTP.
  - Set the spanning tree mode to MSTP. The default spanning tree mode is MSTP and no configuration is required.
  - Configure an MST region. On Devices A, B, C, and D, map instance 1 to VLAN 10 and VLAN 30 and instance 2 to VLAN 20 and VLAN 40.

- Set the bridge priority of instances 0 and 1 to 4096 on Device A and 8192 on Device B to make Device A become the root bridge of instances 0 and 1.
- Set the bridge priority of instance 2 to 8192 on Device A and 4096 on Device B to make Device B become the root bridge of instance 2.
- On access Devices C and D, instances 0, 1, and 2 use the default bridge priority (32768). Configure ports that connect to user terminals as edge ports so that they do not participate in spanning tree calculation. Enable BPDU guard on the ports.

- Configure monitoring ports for a VRRP group. Configure the uplink port of the master device as the VLAN monitoring port. Configure port GigabitEthernet 0/5 of Device A to monitor VLAN 10 and VLAN 30, and port GigabitEthernet 0/5 of Device B to monitor VLAN 20 and VLAN 40.
  - In interface configuration mode of the uplink port, run the **no switchport** command to configure the monitoring port as an L3 interface and configure an IP address for the port. L3 interfaces do not participate in spanning tree calculation.
  - In switch virtual interface (SVI) configuration mode of a VLAN, run the **vrrp** *group-id* **track** *interface-type interface-number* [*priority decrement*] command to configure a monitoring interface *interface-type interface-number* for the VRRP group *group-id* and VRRP priority change value *priority decrement*. *priority decrement* indicates the VRRP priority change value when the link status of the monitored interface or IP route reachability status changes. When the link is interrupted, the priority is reduced. When the link recovers, the priority is restored. The value range is from 1 to 255 and the default value is **10**.
- Configure priority parameters: The VRRP priority change value needs to be taken into account together with the VRRP priority. In SVI configuration mode of a VLAN, run the **vrrp** *group-id* **priority** *priority* command to configure the VRRP priority. The value range of *priority* is from 1 to 254 and the default value is **100**. The default value of *priority decrement* is **10**. When the monitoring port is down, the VRRP priority is reduced to 90 (that is, 100 – 10).
  - In this example, raise the VRRP priority of VLANs 10 and 30 to 120 on the master device (Device A), use the default priority **100** on Device B, and set *priority decrement* to 30. When monitoring port GigabitEthernet 0/5 of Device A is down due to a fault, the VRRP priority of VLAN 10 and VLAN 30 is reduced by 30 to 90, which is lower than the default priority (100) on Device B. Therefore, data of VLAN 10 and VLAN 30 will be transmitted through Device B. When monitoring port GigabitEthernet 0/5 of Device A recovers, the VRRP priority of VLAN 10 and VLAN 30 is restored to 120, which is greater than the default priority on Device B. Therefore, data of VLAN 10 and VLAN 30 is transmitted through Device A. Then, VLAN 10 and VLAN 30 use Device A as the VRRP master device and Device B as the VRRP backup device.
  - Likewise, raise the VRRP priority of VLAN 20 and VLAN 40 to 120 on Device B and use the default priority (**100**) on Device A.
- Configure VRRP: Add SVIs of VLANs to a VRRP group and configure a virtual IP address for the VRRP group.
- Pay attention to the following when configuring SVI addresses: If the monitoring port is down and the VRRP priorities are the same on two devices after priority reduction, the SVI addresses of a VLAN on the two devices will be compared. A larger SVI address indicates a higher priority. Therefore, it is recommended that the SVI IP addresses of VLAN 10 and VLAN 30 on the master device (Device A) be greater than those of VLAN 10 and VLAN 30 on Device B. The same configuration applies to other VLANs.

- Configure an aggregate link between core devices. Configure the downlink ports of core devices and uplink ports of access devices as trunk ports. On access devices, configure ports that connect to user terminals as access ports and add them to VLANs.

4. Procedure

(1) Configure the MSTP function.

Configure the MSTP function for core Device A. Create VLANs, and map instance 1 to VLAN 10 and VLAN 30 and instance 2 to VLAN 20 and VLAN 40. Set the bridge priority to 4096 for instances 0 and 1 and 8192 for instance 2 to make Device A become the root bridge of instances 0 and 1. Enable MSTP.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan range 10,20,30,40
DeviceA(config-vlan-range)# exit
DeviceA(config)# spanning-tree mode mstp
DeviceA(config)# spanning-tree mst configuration
DeviceA(config-mst)# instance 1 vlan 10,30
DeviceA(config-mst)# instance 2 vlan 20,40
DeviceA(config-mst)# exit
DeviceA(config)# spanning-tree mst 0 priority 4096
DeviceA(config)# spanning-tree mst 1 priority 4096
DeviceA(config)# spanning-tree mst 2 priority 8192
DeviceA(config)# spanning-tree
```

Configure the MSTP function for core Device B. Create VLANs, and map instance 1 to VLAN 10 and VLAN 30 and instance 2 to VLAN 20 and VLAN 40. Set the bridge priority to 8192 for instances 0 and 1 and 4096 for instance 2 to make Device B become the root bridge of instance 2. Enable MSTP.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan range 10,20,30,40
DeviceB(config-vlan-range)# exit
DeviceB(config)# spanning-tree mode mstp
DeviceB(config)# spanning-tree mst configuration
DeviceB(config-mst)# instance 1 vlan 10,30
DeviceB(config-mst)# instance 2 vlan 20,40
DeviceB(config-mst)# exit
DeviceB(config)# spanning-tree mst 0 priority 8192
DeviceB(config)# spanning-tree mst 1 priority 8192
DeviceB(config)# spanning-tree mst 2 priority 4096
DeviceB(config)# spanning-tree
```

Configure the MSTP function for access Devices C and D. The bridge priority does not need to be configured on access devices. Configure ports that are directly connected to user terminals as edge ports and enable BPDU guard on the ports. The configurations on Device D are similar to those on Device C. The following uses Device C as an example.

```
DeviceC> enable
DeviceC# configure terminal
```

```
DeviceC(config)# vlan range 10,20,30,40
DeviceC(config-vlan-range)# exit
DeviceC(config)# spanning-tree mode mstp
DeviceC(config)# spanning-tree mst configuration
DeviceC(config-mst)# instance 1 vlan 10,30
DeviceC(config-mst)# instance 2 vlan 20,40
DeviceC(config-mst)# exit
DeviceC(config)# spanning-tree
DeviceC(config)# interface range gigabitethernet 0/3-6
DeviceC(config-if-range)# spanning-tree portfast
DeviceC(config-if-range)# spanning-tree bpduguard enable
DeviceC(config-if-range)# exit
```

(2) Configure monitoring ports for the VRRP group.

Configure port GigabitEthernet 0/5 of Device A as a routing port and set the IP address to 10.10.1.1/24. Then, this port serves as the monitoring port of VLAN 10 and VLAN 30.

```
DeviceA(config)# interface gigabitethernet 0/5
DeviceA(config-if-GigabitEthernet 0/5)# no switchport
DeviceA(config-if-GigabitEthernet 0/5)# ip address 10.10.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/5)# exit
```

Configure port GigabitEthernet 0/5 of Device B as a routing port and set the IP address to 10.10.2.1/24. Then, this port serves as the monitoring port of VLAN 20 and VLAN 40.

```
DeviceB(config)# interface gigabitethernet 0/5
DeviceB(config-if-GigabitEthernet 0/5)# no switchport
DeviceB(config-if-GigabitEthernet 0/5)# ip address 10.10.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/5)# exit
```

(3) Configure VRRP for VLAN 10 and VLAN 30 on core devices.

Configure the master device (Device A). Enter an SVI and configure an SVI address. Add the SVI to the VRRP group and configure a virtual gateway IP address for the VRRP group. Raise the VRRP priority to 120, configure port GigabitEthernet 0/5 as a monitoring port, and set priority decrement to 30.

```
DeviceA(config)# interface vlan 10
DeviceA(config-if-VLAN 10)# ip address 192.168.10.3 255.255.255.0
DeviceA(config-if-VLAN 10)# vrrp 10 ip 192.168.10.1
DeviceA(config-if-VLAN 10)# vrrp 10 priority 120
DeviceA(config-if-VLAN 10)# vrrp 10 track gigabitethernet 0/5 30
DeviceA(config-if-VLAN 10)# exit
DeviceA(config)# interface vlan 30
DeviceA(config-if-VLAN 30)# ip address 192.168.30.3 255.255.255.0
DeviceA(config-if-VLAN 30)# vrrp 30 ip 192.168.30.1
DeviceA(config-if-VLAN 30)# vrrp 30 priority 120
DeviceA(config-if-VLAN 30)# vrrp 30 track gigabitethernet 0/5 30
DeviceA(config-if-VLAN 30)# exit
```

Configure the backup device (Device B). Enter an SVI and configure an SVI address. Add the SVI to the VRRP group and configure a virtual gateway IP address for the VRRP group. On the backup device, use the default VRRP priority (100). No monitoring port needs to be configured.

```
DeviceB(config)# interface vlan 10
DeviceB(config-if-VLAN 10)# ip address 192.168.10.2 255.255.255.0
DeviceB(config-if-VLAN 10)# vrrp 10 ip 192.168.10.1
DeviceB(config-if-VLAN 10)# exit
DeviceB(config)# interface vlan 30
DeviceB(config-if-VLAN 30)# ip address 192.168.30.2 255.255.255.0
DeviceB(config-if-VLAN 30)# vrrp 30 ip 192.168.30.1
DeviceB(config-if-VLAN 30)# exit
```

(4) Configure VRRP for VLAN 20 and VLAN 40 on core devices.

Configure the master device (Device B). Enter an SVI and configure an SVI address. Add the SVI to the VRRP group and configure a virtual gateway IP address for the VRRP group. Raise the VRRP priority to 120, configure port GigabitEthernet 0/5 as a monitoring port, and set priority decrement to 30.

```
DeviceB(config)# interface vlan 20
DeviceB(config-if-VLAN 20)# ip address 192.168.20.3 255.255.255.0
DeviceB(config-if-VLAN 20)# vrrp 20 ip 192.168.20.1
DeviceB(config-if-VLAN 20)# vrrp 20 priority 120
DeviceB(config-if-VLAN 20)# vrrp 20 track gigabitethernet 0/5 30
DeviceB(config-if-VLAN 20)# exit
DeviceB(config)# interface vlan 40
DeviceB(config-if-VLAN 40)# ip address 192.168.40.3 255.255.255.0
DeviceB(config-if-VLAN 40)# vrrp 40 ip 192.168.40.1
DeviceB(config-if-VLAN 40)# vrrp 40 priority 120
DeviceB(config-if-VLAN 40)# vrrp 40 track gigabitethernet 0/5 30
DeviceB(config-if-VLAN 40)# exit
```

Configure the backup device (Device A). Enter an SVI and configure an SVI address. Add the SVI to the VRRP group and configure a virtual gateway IP address for the VRRP group. On the backup device, use the default VRRP priority (100). No monitoring port needs to be configured.

```
DeviceA(config)# interface vlan 20
DeviceA(config-if-VLAN 20)# ip address 192.168.20.2 255.255.255.0
DeviceA(config-if-VLAN 20)# vrrp 20 ip 192.168.20.1
DeviceA(config-if-VLAN 20)# exit
DeviceA(config)# interface vlan 40
DeviceA(config-if-VLAN 40)# ip address 192.168.40.2 255.255.255.0
DeviceA(config-if-VLAN 40)# vrrp 40 ip 192.168.40.1
DeviceA(config-if-VLAN 40)# exit
```

(5) Configure an aggregate link between VRRP core devices.

On Device A, configure ports GigabitEthernet 0/3 and 0/4 as AggregatePort 1 and set the aggregate port to work in trunk mode.

```
DeviceA(config)# interface range gigabitethernet 0/3-4
DeviceA(config-if-range)# port-group 1
DeviceA(config-if-range)# exit
DeviceA(config-if-range)# interface aggregateport 1
DeviceA(config-if-AggregatePort 1)# switchport mode trunk
DeviceA(config-if-AggregatePort 1)# exit
```

On Device B, configure ports GigabitEthernet 0/3 and 0/4 as AggregatePort 1 and set the aggregate port to work in trunk mode.

```
DeviceB(config)# interface range gigabitethernet 0/3-4
DeviceB(config-if-range)# port-group 1
DeviceB(config-if-range)# exit
DeviceB(config-if-range)# interface aggregateport 1
DeviceB(config-if-AggregatePort 1)# switchport mode trunk
DeviceB(config-if-AggregatePort 1)# exit
```

(6) Configure the downlink ports of core devices and the uplink ports of access devices as trunk ports.

Configure downlink ports GigabitEthernet 0/1–0/2 of Device A as trunk ports.

```
DeviceA(config)# interface range gigabitethernet 0/1-2
DeviceA(config-if-range)# switchport mode trunk
DeviceA(config-if-range)# end
DeviceA# write
```

Configure downlink ports GigabitEthernet 0/1–0/2 of Device B as trunk ports.

```
DeviceB(config)# interface range gigabitethernet 0/1-2
DeviceB(config-if-range)# switchport mode trunk
DeviceB(config-if-range)# end
DeviceB# write
```

Configure uplink ports GigabitEthernet 0/1–0/2 of Device C as trunk ports.

```
DeviceC(config)# interface range gigabitethernet 0/1-2
DeviceC(config-if-range)# switchport mode trunk
DeviceC(config-if-range)# exit
```

Configure uplink ports GigabitEthernet 0/1–0/2 of Device D as trunk ports.

```
DeviceD(config)# interface range gigabitethernet 0/1-2
DeviceD(config-if-range)# switchport mode trunk
DeviceD(config-if-range)# exit
```

(7) Set user ports on access devices to work in access mode and add them to VLANs..

Configure Device C.

```
DeviceC(config)# interface gigabitethernet 0/3
DeviceC(config-if-GigabitEthernet 0/3)# switchport mode access
DeviceC(config-if-GigabitEthernet 0/3)# switchport access vlan 10
DeviceC(config-if-GigabitEthernet 0/3)# exit
DeviceC(config)# interface gigabitethernet 0/4
DeviceC(config-if-GigabitEthernet 0/4)# switchport mode access
DeviceC(config-if-GigabitEthernet 0/4)# switchport access vlan 20
DeviceC(config-if-GigabitEthernet 0/4)# exit
DeviceC(config)# interface gigabitethernet 0/5
DeviceC(config-if-GigabitEthernet 0/5)# switchport mode access
DeviceC(config-if-GigabitEthernet 0/5)# switchport access vlan 30
DeviceC(config-if-GigabitEthernet 0/5)# exit
DeviceC(config)# interface gigabitethernet 0/6
DeviceC(config-if-GigabitEthernet 0/6)# switchport mode access
```

```
DeviceC(config-if-GigabitEthernet 0/6)# switchport access vlan 40
DeviceC(config-if-GigabitEthernet 0/6)# end
DeviceC# write
```

Configure Device D.

```
DeviceD(config)# interface gigabitethernet 0/3
DeviceD(config-if-GigabitEthernet 0/3)# switchport mode access
DeviceD(config-if-GigabitEthernet 0/3)# switchport access vlan 10
DeviceD(config-if-GigabitEthernet 0/3)# exit
DeviceD(config)# interface gigabitethernet 0/4
DeviceD(config-if-GigabitEthernet 0/4)# switchport mode access
DeviceD(config-if-GigabitEthernet 0/4)# switchport access vlan 20
DeviceD(config-if-GigabitEthernet 0/4)# exit
DeviceD(config)# interface gigabitethernet 0/5
DeviceD(config-if-GigabitEthernet 0/5)# switchport mode access
DeviceD(config-if-GigabitEthernet 0/5)# switchport access vlan 30
DeviceD(config-if-GigabitEthernet 0/5)# exit
DeviceD(config)# interface gigabitethernet 0/6
DeviceD(config-if-GigabitEthernet 0/6)# switchport mode access
DeviceD(config-if-GigabitEthernet 0/6)# switchport access vlan 40
DeviceD(config-if-GigabitEthernet 0/6)# end
DeviceD# write
```

5. Verification

On Device A, run the **show spanning-tree summary** command to display the spanning tree topology.

```
DeviceA# show spanning-tree summary
Spanning tree enabled protocol mstp

MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID    Priority    4096
           Address     00d0.f822.3344
           this bridge is root
           Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority    4096
           Address     00d0.f822.3344
           Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1            Desg FWD 19000     128     False    P2p
Gi0/1           Desg FWD 200000    128     False    P2p
Gi0/2           Desg FWD 200000    128     False    P2p

MST 1 vlans map : 10,30
  Region Root Priority   4096
```

```
          Address    00d0.f822.3344
          this bridge is region root

  Bridge ID  Priority   4096
          Address    00d0.f822.3344

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1            Desg FWD 19000     128     False    P2p
Gi0/1          Desg FWD 200000    128     False    P2p
Gi0/2          Desg FWD 200000    128     False    P2p

MST 2 vlans map : 20,40
  Region Root Priority   4096
          Address    001a.a917.78cc
          this bridge is region root

  Bridge ID  Priority   8192
          Address    00d0.f822.3344

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1            Root FWD 19000     128     False    P2p
Gi0/1          Desg FWD 200000    128     False    P2p
Gi0/2          Desg FWD 200000    128     False    P2p
```

On Device B, run the **show spanning-tree summary** command to display the spanning tree topology.

```
DeviceB# show spanning-tree summary

Spanning tree enabled protocol mstp

MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID   Priority   4096
          Address    00d0.f822.3344
          this bridge is root
          Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority   8192
          Address    001a.a917.78cc
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1            Root FWD 19000     128     False    P2p
Gi0/1          Desg FWD 200000    128     False    P2p
Gi0/2          Desg FWD 200000    128     False    P2p
```

```
MST 1 vlans map : 10,30
  Region Root Priority   4096
           Address    00d0.f822.3344
           this bridge is region root

  Bridge ID  Priority   8192
           Address    001a.a917.78cc

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1            Root FWD 19000     128     False    P2p
Gi0/1           Desg FWD 200000    128     False    P2p
Gi0/2           Desg FWD 200000    128     False    P2p

MST 2 vlans map : 20,40
  Region Root Priority   4096
           Address    001a.a917.78cc
           this bridge is region root

  Bridge ID  Priority   4096
           Address    001a.a917.78cc

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1            Desg FWD 19000     128     False    P2p
Gi0/1           Desg FWD 200000    128     False    P2p
Gi0/2           Desg FWD 200000    128     False    P2p
```

On Devices C and D, run the **show spanning-tree summary** command to check whether the spanning tree topology is correctly calculated. The following uses Device C as an example.

```
DeviceC# show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID    Priority   4096
           Address    00d0.f822.3344
           this bridge is root
           Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority   32768
           Address    001a.a979.00ea
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    Type  OperEdge
---------------- ---- --- ---------- -------- ----- ----------------
Gi0/2           Altn BLK 200000    128     P2p   False
Gi0/1           Root FWD 200000    128     P2p   False
```

```
MST 1 vlans map : 10,30
  Region Root Priority   4096
           Address    00d0.f822.3344
           this bridge is region root

  Bridge ID  Priority   32768
           Address    001a.a979.00ea

Interface       Role Sts Cost      Prio    Type  OperEdge
---------------- ---- --- ---------- -------- ----- ---------------
Gi0/2           Altn BLK 200000    128     P2p   False
Gi0/1           Root FWD 200000    128     P2p   False

MST 2 vlans map : 20,40
  Region Root Priority   4096
           Address    001a.a917.78cc
           this bridge is region root

  Bridge ID  Priority   32768
           Address    001a.a979.00ea

Interface       Role Sts Cost      Prio    Type  OperEdge
---------------- ---- --- ---------- -------- ----- ---------------
Gi0/2           Root FWD 200000    128     P2p   False
Gi0/1           Altn BLK 200000    128     P2p   False
```

On Devices A and B, run the **show vrrp brief** command to check whether VRRP master/slave relationship is successfully established.

```
DeviceA# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   120  3      -    P    Master  192.168.10.3  192.168.10.1
VLAN 20    20   100  3      -    P    Backup  192.168.20.2  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -    P    Backup  192.168.40.2  192.168.40.1

DeviceB# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Backup  192.168.10.2  192.168.10.1
VLAN 20    20   120  3      -    P    Master  192.168.20.3  192.168.20.1
VLAN 30    30   100  3      -    P    Backup  192.168.30.2  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
```

Disconnect uplink GigabitEthernet 0/5 of Device A and check the VRRP status change on Device A and Device B.

```
DeviceA#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
```

```
VLAN 10    10   90    3      -   P    Backup  192.168.10.3  192.168.10.1
VLAN 20    20   100   3      -   P    Backup  192.168.20.2  192.168.20.1
VLAN 30    30   90   3      -   P    Backup  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -   P    Backup  192.168.40.2  192.168.40.1

DeviceB# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Master  192.168.10.2  192.168.10.1
VLAN 20    20   120  3      -    P    Master  192.168.20.3  192.168.20.1
VLAN 30    30   100  3      -    P    Master  192.168.30.2  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
```

Disconnect uplink GigabitEthernet 0/5 of Device B and check the VRRP status change on Device A and Device B.

```
DeviceA# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   120  3      -    P    Master  192.168.10.3  192.168.10.1
VLAN 20    20   100  3      -    P    Master  192.168.20.2  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -    P    Master  192.168.40.2  192.168.40.1

DeviceB# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Backup  192.168.10.2  192.168.10.1
VLAN 20    20   90   3      -    P    Backup  192.168.20.3  192.168.20.1
VLAN 30    30   100  3      -    P    Backup  192.168.30.2  192.168.30.1
VLAN 40    40   90   3      -    P    Backup  192.168.40.3  192.168.40.1
```

6. Configuration Files

- Device A configuration file

```
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 30
 instance 2 vlan 20, 40
!
spanning-tree mst 0 priority 4096
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
spanning-tree
!
sysmac 00d0.f822.3344
!
vlan range 1,10,20,30,40
!
interface GigabitEthernet 0/1
 switchport mode trunk
```

```
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface GigabitEthernet 0/3
 port-group 1
!
interface GigabitEthernet 0/4
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface gigabitethernet 0/5
 no switchport
 ip address 10.10.1.1 255.255.255.0
!
interface vlan 10
 ip address 192.168.10.3 255.255.255.0
 vrrp 10 ip 192.168.10.1
 vrrp 10 priority 120
 vrrp 10 track gigabitethernet 0/5 30
!
interface vlan 20
 ip address 192.168.20.2 255.255.255.0
 vrrp 20 ip 192.168.20.1
!
interface vlan 30
 ip address 192.168.30.3 255.255.255.0
 vrrp 30 ip 192.168.30.1
 vrrp 30 priority 120
 vrrp 30 track gigabitethernet 0/5 30
!
interface vlan 40
 ip address 192.168.40.2 255.255.255.0
 vrrp 40 ip 192.168.40.1
```

- Device B configuration file

```
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 30
 instance 2 vlan 20, 40
!
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
spanning-tree
```

```
!
sysmac 001a.a917.78cc
!
vlan range 1,10,20,30,40
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface GigabitEthernet 0/3
 port-group 1
!
interface GigabitEthernet 0/4
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface gigabitethernet 0/5
 no switchport
 ip address 10.10.2.1 255.255.255.0
!
interface vlan 10
 ip address 192.168.10.2 255.255.255.0
 vrrp 10 ip 192.168.10.1
!
interface vlan 20
 ip address 192.168.20.3 255.255.255.0
 vrrp 20 ip 192.168.20.1
 vrrp 20 priority 120
 vrrp 20 track gigabitethernet 0/5 30
!
interface vlan 30
 ip address 192.168.30.2 255.255.255.0
 vrrp 30 ip 192.168.30.1
!
interface vlan 40
 ip address 192.168.40.3 255.255.255.0
 vrrp 40 ip 192.168.40.1
 vrrp 40 priority 120
 vrrp 40 track gigabitethernet 0/5 30
```

- Configuration files of Devices C and D

```
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
```

```
 instance 1 vlan 10, 30
 instance 2 vlan 20, 40
!
spanning-tree
!
vlan range 1,10,20,30,40
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface GigabitEthernet 0/3
 switchport access vlan 10
 spanning-tree bpduguard enable
 spanning-tree portfast
!
interface GigabitEthernet 0/4
 switchport access vlan 20
 spanning-tree bpduguard enable
 spanning-tree portfast
!
interface GigabitEthernet 0/5
 switchport access vlan 30
 spanning-tree bpduguard enable
 spanning-tree portfast
!
interface GigabitEthernet 0/6
 switchport access vlan 40
 spanning-tree bpduguard enable
 spanning-tree portfast
```

7. Common Errors

- In the MSTP+VRRP topology, the MST region configurations on different devices are different.
- VLANs are not created before the mappings between instances and VLANs are configured.
- In the MSTP+VRRP topology, if some devices run STP or RSTP, the devices will be considered as different MST regions for spanning tree calculation. In this case, the calculated spanning tree will be different from expectations.

1.21.3 Configuring Spanning Tree Compatibility for MSTP Interfaces

1. Requirements

In the topology as shown in Figure 1-20, enable MSTP on Device A and Device B and configure the same instance mappings on the devices: Associate instance 1 with VLAN 10 and add port GigabitEthernet 0/1 to VLAN 10; associate instance 2 with VLAN 20 and add port GigabitEthernet 0/2 to VLAN 20. Configure spanning

tree compatibility for interfaces so that BPDUs sent by interfaces carry only information about instances corresponding to the VLANs, to which the interfaces belong.

2. Topology

Figure 1-20 Basic Configuration

3. Notes

- Adopt the same configurations on Device A and Device B. The following uses Device A as an example.
- Create VLAN 10, VLAN 20, instance 1, and instance 2. Associate instance 1 with VLAN 10 and instance 2 with VLAN 20. Add port GigabitEthernet 0/1 to VLAN 10 and port GigabitEthernet 0/2 to VLAN 20, and configure spanning tree compatibility for the ports. Enable the STP function.

4. Procedure

(1) Create VLAN 10, VLAN 20, instance 1, and instance 2. Associate instance 1 with VLAN 10 and instance 2 with VLAN 20.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan range 10,20
DeviceA(config-vlan-range)# exit
DeviceA(config)# spanning-tree mst configuration
DeviceA(config-mst)# instance 1 vlan 10
DeviceA(config-mst)# instance 2 vlan 20
DeviceA(config-mst)# exit
```

(2) Add port GigabitEthernet 0/1 to VLAN 10 and port GigabitEthernet 0/2 to VLAN 20, and configure spanning tree compatibility for the ports.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport access vlan 10
DeviceA(config-if-GigabitEthernet 0/1)# spanning-tree compatible enable
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# switchport access vlan 20
DeviceA(config-if-GigabitEthernet 0/2)# spanning-tree compatible enable
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

(3) Enable the STP function.

```
DeviceA(config)# spanning-tree
DeviceA(config)# end
DeviceA# write
```

5. Verification

(1) If no spanning tree compatibility is configured for interfaces, check the spanning tree configuration as follows.

Device A becomes the root of Device B because its bridge ID is smaller. Ports GigabitEthernet 0/1 and GigabitEthernet 0/2 of Device A are designated ports in their respective instances.

```
DeviceA# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID    Priority    32768
           Address     0074.9cee.53ca
           this bridge is root
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
           Address     0074.9cee.53ca
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Desg FWD 20000     128     False    P2p
Gi0/2           Desg FWD 20000     128     False    P2p

MST 1 vlans map : 10
  Region Root Priority   32768
           Address     0074.9cee.53ca
           this bridge is region root

  Bridge ID  Priority    32768
           Address     0074.9cee.53ca

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Desg FWD 20000     128     False    P2p
Gi0/2           Desg FWD 20000     128     False    P2p

MST 2 vlans map : 20
  Region Root Priority   32768
           Address     0074.9cee.53ca
           this bridge is region root

  Bridge ID  Priority    32768
           Address     0074.9cee.53ca

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
```

```
Gi0/1          Desg FWD 20000    128     False   P2p
Gi0/2          Desg FWD 20000     128     False   P2p
```

Check Device B. In the spanning tree of instance 1, port GigabitEthernet 0/1 belonging to VLAN 10 is the root port and port GigabitEthernet 0/2 belonging to VLAN 20 is the alternate port. Port GigabitEthernet 0/2 rejects traffic of VLAN 10 to pass. Therefore, the alternate port cannot serve as an alternative to the root port. In the spanning tree of instance 2, port GigabitEthernet 0/2 belonging to VLAN 20 is the root port and port GigabitEthernet 0/1 belonging to VLAN 10 is the alternate port. Port GigabitEthernet 0/1 rejects traffic of VLAN 20 to pass. Therefore, the alternate port cannot serve as an alternative to the root port.

```
DeviceB# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID   Priority   32768
           Address    0074.9cee.53ca
           this bridge is root
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority   32768
           Address    0074.9cee.f49e
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1          Root FWD 20000     128     False   P2p
Gi0/2          Altn BLK 20000     128     False   P2p

MST 1 vlans map : 10
  Region Root Priority  32768
           Address    0074.9cee.53ca
           this bridge is region root

  Bridge ID  Priority   32768
           Address    0074.9cee.f49e

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1          Root FWD 20000     128     False   P2p
Gi0/2          Altn BLK 20000     128     False   P2p

MST 2 vlans map : 20
  Region Root Priority  32768
           Address    0074.9cee.53ca
           this bridge is region root

  Bridge ID  Priority   32768
           Address    0074.9cee.f49e
```

```
Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Altn BLK 20000     128     False    P2p
Gi0/2           Root FWD 20000     128     False    P2p
```

(2) After spanning tree compatibility is configured for interfaces, check the spanning tree topology on Device A. Device A becomes the root of Device B because its bridge ID is smaller.

The spanning tree is not pruned in instance 0. Ports GigabitEthernet 0/1 and GigabitEthernet 0/2 are designated ports.

```
DeviceA# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID    Priority    32768
           Address     0074.9cee.53ca
           this bridge is root
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
           Address     0074.9cee.53ca
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Desg FWD 20000     128     False    P2p
Gi0/2           Desg FWD 20000     128     False    P2p
```

The spanning tree is pruned in instance 1. Only port GigabitEthernet 0/1 belonging to VLAN 10 is the designated port.

```
MST 1 vlans map : 10
  Region Root Priority   32768
           Address     0074.9cee.53ca
           this bridge is region root

  Bridge ID  Priority    32768
           Address     0074.9cee.53ca

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Desg FWD 20000     128     False    P2p
```

The spanning tree is pruned in instance 2. Only port GigabitEthernet 0/2 belonging to VLAN 20 is the designated port.

```
MST 2 vlans map : 20
  Region Root Priority   32768
           Address     0074.9cee.53ca
           this bridge is region root
```

```
  Bridge ID  Priority    32768
           Address     0074.9cee.53ca

Interface        Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2           Desg FWD 20000     128     False    P2p
```

(3) Check the spanning tree topology on Device B. Device A becomes the root of Device B because its bridge ID is smaller.

The spanning tree is not pruned in instance 0. Port GigabitEthernet 0/1 is the root port and port GigabitEthernet 0/2 is the alternate port.

```
DeviceB# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID    Priority    32768
           Address     0074.9cee.53ca
           this bridge is root
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
           Address     0074.9cee.f49e
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface        Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Root FWD 20000     128     False    P2p
Gi0/2           Altn BLK 20000     128     False    P2p
```

The spanning tree is pruned in instance 1. Only port GigabitEthernet 0/1 belonging to VLAN 10 is the root port and there is no alternate port.

```
MST 1 vlans map : 10
  Region Root Priority   32768
           Address     0074.9cee.53ca
           this bridge is region root

  Bridge ID  Priority    32768
           Address     0074.9cee.f49e

Interface        Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Root FWD 20000     128     False    P2p
```

The spanning tree is pruned in instance 2. Only port GigabitEthernet 0/2 belonging to VLAN 20 is the root port and there is no alternate port.

```
MST 2 vlans map : 20
  Region Root Priority   32768
```

```
          Address    0074.9cee.53ca
          this bridge is region root

  Bridge ID  Priority    32768
          Address    0074.9cee.f49e

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2           Root FWD 20000     128     False    P2p
```

6. Configuration Files

Configuration files of Devices A and B

```
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-4094
 instance 1 vlan 10
 instance 2 vlan 20
!
spanning-tree
!
vlan range 1,10,20
!
interface GigabitEthernet 0/1
 switchport access vlan 10
 spanning-tree compatible enable
!
interface GigabitEthernet 0/2
 switchport access vlan 20
 spanning-tree compatible enable
```

7. Common Errors

- If the VLAN lists configured on interfaces at both ends of a link are inconsistent, communication may fail after VLANs are pruned by the spanning tree compatibility function of the interfaces.
- If different instances are not configured or interfaces permit the traffic of all VLANs to pass, the spanning tree compatibility function cannot perform spanning tree pruning based on instances. In this case, there is no necessary to configure the spanning tree compatibility function.

1.21.4 Configuring BPDU Tunnel

1. Requirements

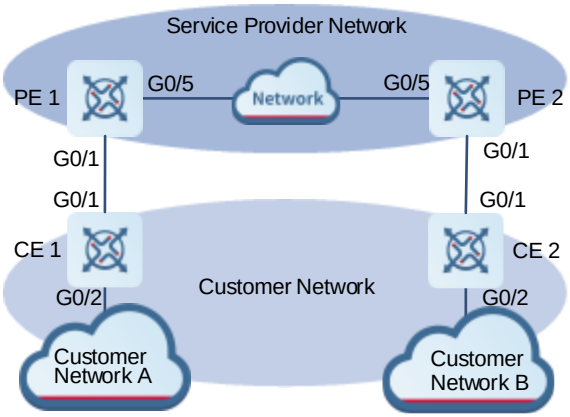
In the typical QinQ network topology shown in Figure 1-21, the upper part is the service provider network while the lower part is the customer network. The service provider network consists of two PEs: PE 1 and PE 2. Customer Network A and Customer Network B are two sites of the same customer in different regions. CE 1 and CE 2 are access devices for connecting the customer networks to the service provider network, and they connect to the service provider network respectively through PE 1 and PE 2.

Configure an L2 protocol tunnel to transparently transmit L2 protocol packets from the customer network at one end to the customer network at the other end so that the spanning trees of the customer network and

service provider network are separately calculated without interference. According to the needs of the customer, configure the STP tunnel function to transmit BPDUs from the customer network through a tunnel in the service provider network so that the spanning tree is calculated in a unified manner for the cross-region customer network, independent of the service provider network.

2. Topology

Figure 1-21 BPDU Tunnel Application Topology



3. Notes

- Configure MSTP on PE 1 and PE 2. Configure the bridge priority to make PE 1 become the root of instances 0 and 1, and PE 2 the root of instance 2. Enable STP.
- Configure the QinQ encapsulation mode (for example, basic QinQ) on PE 1 and PE 2. Configure VLAN 10 as the native VLAN of tunnel ports and add VLAN 10 to the permitted untagged VLAN list of the tunnel ports. Configure VLAN 10 as the public network transmission channel. VLAN 10 is encapsulated into the user data packets before they are forwarded in the public network. Configure port GigabitEthernet 0/1 as a tunnel port and enable the STP tunnel function. Enable the global STP tunnel function.
- Configure the uplink ports of PE 1 and PE 2 as the uplink ports.
- Configure STP on CE 1 and CE 2. Set the bridge priority to 0, configure timer parameters, and enable STP on CE 1.
- Configure the uplink and downlink ports of CE 1 and CE 2 as trunk ports.

4. Procedure

(1) Configure MSTP on PE 1 and PE 2.

Set the bridge priority to 4094 for instances 0 and 1 and 8192 for instance 2 on PE 1.

```
PE1> enable
PE1# configure terminal
PE1(config)# vlan range 10,20,30,40
PE1(config-vlan-range)# exit
PE1(config)# spanning-tree mst configuration
PE1(config-mst)# instance 1 vlan 10,30
PE1(config-mst)# instance 2 vlan 20,40
PE1(config-mst)# spanning-tree mst 0 priority 4096
```

```
PE1(config)# spanning-tree mst configuration
PE1(config-mst)# spanning-tree mst 1 priority 4096
PE1(config)# spanning-tree mst configuration
PE1(config-mst)# spanning-tree mst 2 priority 8192
PE1(config)# spanning-tree
```

Set the bridge priority to 4094 for instance 2 and 8192 for instances 0 and 1 on PE 2.

```
PE2> enable
PE2# configure terminal
PE2(config)# vlan range 10,20,30,40
PE2(config-vlan-range)# exit
PE2(config)# spanning-tree mst configuration
PE2(config-mst)# instance 1 vlan 10,30
PE2(config-mst)# instance 2 vlan 20,40
PE2(config-mst)# spanning-tree mst 0 priority 8192
PE2(config)# spanning-tree mst configuration
PE2(config-mst)# spanning-tree mst 1 priority 8192
PE2(config)# spanning-tree mst configuration
PE2(config-mst)# spanning-tree mst 2 priority 4096
PE2(config)# spanning-tree
```

(2) Configure the basic QinQ transmission channel VLAN 10 on PE 1 and PE 2. Enable the interface STP tunnel function and global STP tunnel function. The configurations on PE 1 are the same as those on PE 2. The following uses PE 1 as an example.

```
PE1(config)# interface gigabitethernet 0/1
PE1(config-if-GigabitEthernet 0/1)# switchport
PE1(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
PE1(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel native vlan 10
PE1(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan add
untagged 10
PE1(config-if-GigabitEthernet 0/1)# l2protocol-tunnel stp enable
PE1(config-if-GigabitEthernet 0/1)# exit
PE1(config)# l2protocol-tunnel stp
```

(3) Configure the uplink ports of PE 1 and PE 2 as the uplink ports. The configurations on PE 1 are the same as those on PE 2. The following uses PE 1 as an example.

```
PE1(config)# interface gigabitethernet 0/5
PE1(config-if-GigabitEthernet 0/5)# switchport
PE1(config-if-GigabitEthernet 0/5)# switchport mode uplink
PE1(config-if-GigabitEthernet 0/5)# end
PE1# write
```

(4) Configure STP on CE 1 and CE 2.

Set the spanning tree mode to STP and bridge priority to 0, configure timer parameters, and enable STP on CE 1.

```
CE1> enable
CE1# configure terminal
CE1(config)# spanning-tree mode stp
```

```
CE1(config)# spanning-tree priority 0
CE1(config)# spanning-tree hello-time 4
CE1(config)# spanning-tree max-age 25
CE1(config)# spanning-tree forward-time 18
CE1(config)# spanning-tree
```

Set the spanning tree mode to STP and enable STP on CE 2.

```
CE2> enable
CE2# configure terminal
CE2(config)# spanning-tree mode stp
CE2(config)# spanning-tree
```

(5) Configure the uplink and downlink ports of CE 1 and CE 2 as trunk ports. The configurations on CE 1 are the same as those on CE 2. The following uses CE 1 as an example.

```
CE1(config)# interface range gigabitethernet 0/1-2
CE1(config-if-range)# switchport
CE1(config-if-range)# switchport mode trunk
CE1(config-if-range)# end
CE1# write
```

5. Verification

(1) Check tunnel port configurations on PE 1 and PE 2. The configurations on PE 1 are the same as those on PE 2. The following uses PE 1 as an example.

```
PE1# show interfaces dot1q-tunnel
========Interface Gi0/1========
Native vlan: 10
Allowed vlan list:1,10,
Tagged vlan list:
```

(2) Verify that the STP tunnel function is enabled in both global configuration mode and interface configuration mode on PE 1 and PE 2. The configurations on PE 1 are the same as those on PE 2. The following uses PE 1 as an example.

```
PE1# show l2protocol-tunnel stp
L2protocol-tunnel: Stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
GigabitEthernet 0/1 l2protocol-tunnel stp enable
```

(3) Check that PE 1 and PE 2 have independent spanning tree topologies.

Check the spanning tree topology on PE 1. For instances 0 and 1, PE 1 is the root of PE 2 and port GigabitEthernet 0/5 is the designated port. For instance 2, PE 2 is the root of PE 1 and port GigabitEthernet 0/5 is the root port. Port GigabitEthernet 0/1 that connects to CE 1 of the customer network is not included in the spanning tree topologies of PE 1 and PE 2. The spanning tree time parameters (**Hello Time**: **2 sec**; **Forward Delay**: **15 sec**; **Max Age**: **20 sec**) of PE 1 use default values and are not affected by the configurations of CE 1.

```
PE1# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
```

```
  Root ID   Priority   4096
           Address    0074.9cee.f49e
           this bridge is root
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority   4096
           Address    0074.9cee.f49e
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/5          Desg FWD 20000     128     False   P2p

MST 1 vlans map : 10, 30
  Region Root Priority   4096
           Address    0074.9cee.f49e
           this bridge is region root

  Bridge ID  Priority   4096
           Address    0074.9cee.f49e

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/5          Desg FWD 20000     128     False   P2p

MST 2 vlans map : 20, 40
  Region Root Priority   4096
           Address    00d0.f8ee.8c1e
           this bridge is region root

  Bridge ID  Priority   8192
           Address    0074.9cee.f49e

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/5          Root FWD 20000        128     False   P2p
```

Check the spanning tree topology on PE 2. For instances 0 and 1, PE 1 is the root of PE 2 and port GigabitEthernet 0/5 is the root port. For instance 2, PE 2 is the root of PE 1 and port GigabitEthernet 0/5 is the designated port. Port GigabitEthernet 0/1 that connects to CE 2 of the customer network is not included in the spanning tree topologies of PE 1 and PE 2. The spanning tree time parameters (**Hello Time**: **2 sec**; **Forward Delay**: **15 sec**; **Max Age**: **20 sec**) of PE 2 use default values and are not affected by the configurations of CE 1.

```
PE2# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
```

```
  Root ID   Priority   4096
            Address    0074.9cee.f49e
            this bridge is root
            Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority   8192
            Address    00d0.f8ee.8c1e
            Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/5           Root FWD 20000        128     False    P2p

MST 1 vlans map : 10, 30
  Region Root Priority   4096
            Address    0074.9cee.f49e
            this bridge is region root

  Bridge ID  Priority   8192
            Address    00d0.f8ee.8c1e

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/5           Root FWD 20000        128     False    P2p

MST 2 vlans map : 20, 40
  Region Root Priority   4096
            Address    00d0.f8ee.8c1e
            this bridge is region root

  Bridge ID  Priority   4096
            Address    00d0.f8ee.8c1e

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/5           Desg FWD 20000     128     False    P2p
```

(4) Check that CE 1 and CE 2 have independent spanning tree topologies.

Check the spanning tree topology on CE 1. CE 1 is the root of CE 2 and port GigabitEthernet 0/1 of CE 1 is the designated port. The spanning tree time parameters (**Hello Time**: **4 sec**; **Forward Delay**: **18 sec**; **Max Age**: **25 sec**) of CE 1 use configured values.

```
CE1# show spanning-tree summary
Spanning tree enabled protocol stp
  Root ID   Priority   0
            Address    0074.9cee.53ca
            this bridge is root
```

```
          Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority    0
          Address    0074.9cee.53ca
          Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1          Desg FWD 20000     128     False    P2p
Gi0/2          Desg FWD 20000     128     False    P2p
```

Check the spanning tree topology on CE 2. CE 1 is the root of CE 2 and port GigabitEthernet 0/1 of CE 2 is the root port. The spanning tree time parameters (**Hello Time**: **4 sec**; **Forward Delay**: **18 sec**; **Max Age**: **25 sec**) of CE 2 use configured values of the root CE 1.

```
CE2# show spanning-tree summary
Spanning tree enabled protocol stp
  Root ID    Priority    0
          Address    0074.9cee.53ca
          this bridge is root
          Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority    32768
          Address    0074.9c11.c9e6
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1          Root FWD 20000     128     False    P2p Bound(STP)
Gi0/2          Desg FWD 20000     128     False    P2p
```

6. Configuration Files

- PE 1 configuration file

```
l2protocol-tunnel stp
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 30
 instance 2 vlan 20, 40
!
spanning-tree mst 0 priority 4096
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
spanning-tree
!
sysmac 0074.9cee.f49e
!
vlan range 1,10,20,30,40
```

```
!
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 10
 switchport dot1q-tunnel native vlan 10
 l2protocol-tunnel stp enable
!
interface GigabitEthernet 0/5
 switchport mode uplink
```

- PE 2 configuration file

```
l2protocol-tunnel stp
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 30
 instance 2 vlan 20, 40
!
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
spanning-tree
!
sysmac 00d0.f8ee.8c1e
!
vlan range 1,10,20,30,40
!
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 10
 switchport dot1q-tunnel native vlan 10
 l2protocol-tunnel stp enable
!
interface GigabitEthernet 0/5
 switchport mode uplink
```

- CE 1 configuration file

```
spanning-tree max-age 25
spanning-tree forward-time 18
spanning-tree hello-time 4
spanning-tree mode stp
spanning-tree mst 0 priority 0
spanning-tree
!
sysmac 0074.9cee.53ca
!
interface GigabitEthernet 0/1
 switchport mode trunk
```

```
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

- CE 2 configuration file

```
spanning-tree mode stp
spanning-tree
!
sysmac 0074.9c11.c9e6
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

7. Common Errors

- The L2 protocol tunnel function is not enabled in both global configuration mode and interface configuration mode. As a result, the BPDU tunnel function does not take effect.
- The BPDU tunnel addresses configured in the service provider network are inconsistent. As a result, BPDU frames from the customer network cannot be correctly transmitted.

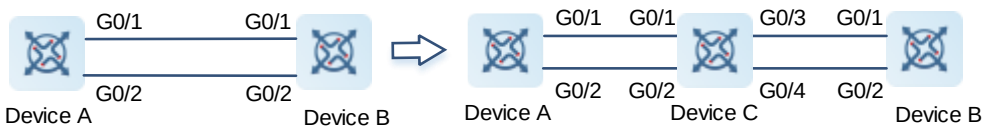
1.21.5 Configuring BPDU Transparent Transmission

1. Requirements

In the topology as shown in Figure 1-22, Device A is connected to Device B and MSTP is enabled on them. Device A is the root of Device B. One Device C with STP disabled is added between Device A and Device B. Configure the BPDU transparent transmission function on Device C to transmit STP packets of Device A and Device B so that Device A and Device B can still conduct calculation together and generate spanning trees.

2. Topology

Figure 1-22 Configuring BPDU Transparent Transmission



3. Notes

- On Device A, configure STP, set the bridge priority to 0 (smaller than the default value **32768**), and set the priority of port GigabitEthernet 0/2 to 16 (smaller than the default value **128**). In this way, Device A becomes the root bridge of Device B and port GigabitEthernet 0/2 of Device B becomes the root port.
- Enable STP on Device B.
- Configure BPDU transparent transmission on Device C.
- Configure interconnected ports as trunk ports.

4. Procedure

(1) On Device A, configure the interconnected ports as trunk ports. Configure the device priority and port priority and enable the STP function.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# spanning-tree mst 0 priority 0
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# switchport
DeviceA(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/2)# spanning-tree mst 0 port-priority 16
DeviceA(config)# spanning-tree
```

(2) On Device B, enable the STP function and configure the interconnected ports as trunk ports.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# spanning-tree
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# switchport
DeviceB(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/1)# exit
DeviceB(config)# interface gigabitethernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# switchport
DeviceB(config-if-GigabitEthernet 0/2)# switchport mode trunk
```

(3) On Device C, configure BPDU transparent transmission and configure the interconnected ports as trunk ports.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# no spanning-tree
DeviceC(config)# bridge-frame forwarding protocol bpdu
DeviceC(config)# interface range gigabitethernet 0/1-4
DeviceC(config-if-rang)# switchport
DeviceC(config-if-rang)# switchport mode trunk
```

5. Verification

(1) When Device C is not connected, check the spanning tree topology.

Check the spanning tree topology of Device A. Device A is the root.

```
DeviceA# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
  Root ID    Priority    0
           Address     0074.9cee.53ca
```

```
          this bridge is root
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    0
          Address    0074.9cee.53ca
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Desg FWD 20000     128     False    P2p
Gi0/2           Desg FWD 20000     16      False    P2p
```

Check the spanning tree topology of Device B. Device A is the root of Device B. The port priority of Device A is changed. Therefore, port GigabitEthernet 0/2 of Device B becomes the root port and port GigabitEthernet 0/1 becomes an alternate port.

```
DeviceB# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
  Root ID    Priority    0
          Address    0074.9cee.53ca
          this bridge is root
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    8192
          Address    00d0.f8ee.8c1e
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Altn BLK 20000     128     False    P2p
Gi0/2           Root FWD 20000     128     False    P2p
```

(2) After Device C is connected to the topology, check the spanning tree topology.

Check the spanning tree topology on Device A. The spanning tree topology of Device A keeps unchanged.

```
DeviceA# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
  Root ID    Priority    0
          Address    0074.9cee.53ca
          this bridge is root
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    0
          Address    0074.9cee.53ca
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
```

```
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Desg FWD 20000     128      False    P2p
Gi0/2           Desg FWD 20000     16       False    P2p
```

Check the spanning tree topology on Device B. Device A is still the root of Device B, but port GigabitEthernet 0/1 of Device B becomes the root port, and port GigabitEthernet 0/2 becomes an alternate port. After Device C is configured to transparently transmit STP packets, ports GigabitEthernet 0/1 and 0/2 of Device B can receive BPDUs from port GigabitEthernet 0/2 of Device A. Therefore, the root port cannot be elected based on the port priority and port GigabitEthernet 0/1 of Device B is elected as the root port because of its smaller port ID.

```
DeviceB# show spanning-tree summary
Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
  Root ID    Priority    0
           Address     0074.9cee.53ca
           this bridge is root
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    8192
           Address     00d0.f8ee.8c1e
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Root FWD 20000     128      False    P2p
Gi0/2           Altn BLK 20000     128      False    P2p
```

6. Configuration Files

- Device A configuration file

```
spanning-tree mst 0 priority 0
spanning-tree
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
 spanning-tree mst 0 port-priority 16
!
```

- Device B configuration file

```
spanning-tree

interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
```

```
 switchport mode trunk
```

- Device C configuration file

```
bridge-frame forwarding protocol bpdu
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface GigabitEthernet 0/3
 switchport mode trunk
!
interface GigabitEthernet 0/4
 switchport mode trunk
```

-

Contents

1 Configuring ERPS 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Control VLAN and Data VLAN 1
1.1.3 Basic Model of an Ethernet Ring 1
1.1.4 RPL and Nodes 3
1.1.5 ERPS Packet 4
1.1.6 ERPS Timer 5
1.1.7 Ring Protection 5
1.1.8 Load Balancing 6
1.1.9 Protocols and Standards 6
1.2 Configuration Task Summary 6
1.3 Configuring a Control VLAN for an Ethernet Ring 7
1.3.1 Overview 7
1.3.2 Restrictions and Guidelines 7
1.3.3 Procedure 7
1.4 Configuring Member Ports for an Ethernet Ring 7
1.4.1 Overview 7
1.4.2 Restrictions and Guidelines 8
1.4.3 Procedure 8
1.5 Configuring an RPL Port 9
1.5.1 Overview 9

1.5.2 Restrictions and Guidelines 9

1.5.3 Procedure 9

1.6 Configuring Major Rings to Associate with Subrings 10

1.6.1 Overview 10

1.6.2 Restrictions and Guidelines 10

1.6.3 Procedure 10

1.7 Configuring Subring Topology Change Notification 10

1.7.1 Overview 10

1.7.2 Procedure 10

1.8 Configuring a Protected VLAN for an Ethernet Ring 11

1.8.1 Overview 11

1.8.2 Restrictions and Guidelines 11

1.8.3 Procedure 11

1.9 Enabling ERPS for an Ethernet Ring 12

1.9.1 Overview 12

1.9.2 Restrictions and Guidelines 12

1.9.3 Procedure 12

1.10 Configuring ERPS Timers 12

1.10.1 Overview 12

1.10.2 Restrictions and Guidelines 12

1.10.3 Procedure 12

1.11 Enabling ERPS Globally 13

1.11.1 Overview 13

1.11.2 Procedure 13

1.12 Monitoring 13

1.13 Configuration Examples..... 14

1.13.1 Configuring Single-Ring Protection 14

1.13.2 Configuring Tangent-Ring Protection..... 17

1.13.3 Configuring Intersecting-Ring Protection..... 22

1.13.4 Configuring Load Balancing..... 29

1.13.5 Modifying ERPS Configuration 34

1 Configuring ERPS

1.1 Introduction

1.1.1 Overview

Ethernet Ring Protection Switching (ERPS), also known as G.8032, is a ring protection protocol developed by the International Telecommunication Union (ITU). It is a data link layer protocol specially designed for Ethernet rings. ERPS prevents broadcast storms caused by data loops when an Ethernet ring network is intact, and can rapidly perform link switching and recover the communication between nodes when a link is disconnected in the Ethernet ring, so as to implement data link redundancy.

Currently, the Spanning Tree Protocol (STP) is another solution to the L2 network loop problem. STP is at mature application stage but requires a relatively long (within seconds) convergence time. Compared with STP, ERPS provides faster convergence, with the L2 convergence time less than 50 ms.

1.1.2 Control VLAN and Data VLAN

ERPS supports two types of virtual local area networks (VLANs): control VLANs and data VLANs.

- Control VLAN: Also known as the Ring Auto Protection Switching VLAN (R-APS VLAN) for transmitting ERPS protocol packets. On a device, the ports connecting to an ERPS ring belong to a control VLAN, and only such ports can be added to a control VLAN.
- Data VLAN: A data VLAN is used to transmit data packets. Both ERPS ports and non-ERPS ports can be assigned to a data VLAN. A data VLAN is also known as a protected VLAN.

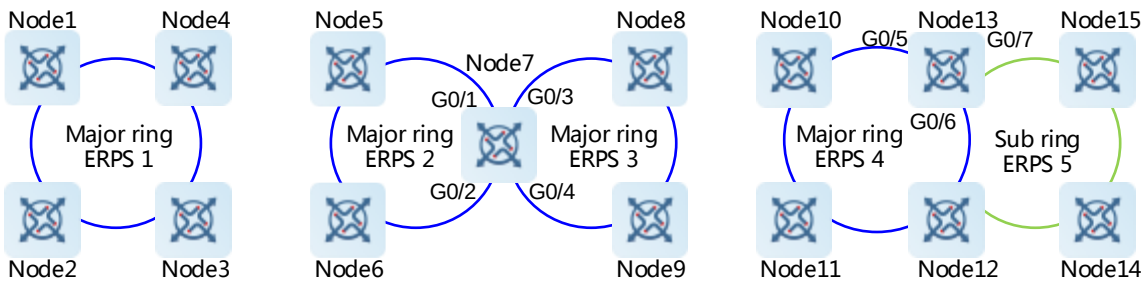
1.1.3 Basic Model of an Ethernet Ring

A group of interconnected devices in the same control VLAN (R-APS VLAN) constitute an Ethernet ring (ERPS ring), in which each device is called a node. ERPS rings can be classified into major rings and subrings based on whether a ring is closed.

1. Major Ring and Subring

- Major ring and major ring link: A major ring is a topology of a closed network connected in a ring, such as the blue rings shown in Figure 1-1. In an ERPS ring, links that belong to and are controlled by a major ring are called major ring links.
- Subring and subring link: A subring is a topology of a non-closed network attached to a major ring, such as the green ring shown in Figure 1-1. In an ERPS ring, links that belong to and are controlled by a subring are called subring links.
- R-APS virtual channel in a subring: A channel used to transmit subring protocol packets in a major ring. It belongs to a major ring rather than a subring. For example, the link between node 12 and node 13 as shown in Figure 1-1 is an R-APS virtual channel.

Figure 1-1 Basic Topologies of Ethernet Rings



2. Basic Topologies

Major rings, subrings, and nodes can form basic topologies with different characteristics, depending on the connection modes, as shown in Figure 1-1.

- Single ring: Major ring ERPS 1 (node 1-2-3-4) constitutes a single-ring topology.
- Tangent rings: A topology in which two ERPS rings share one device is called tangent rings. Major ring ERPS 2 (node 5-6-7) and major ring ERPS 3 (node 7-8-9) constitute a tangent-ring topology, and are tangent to each other on one node, namely, node 7.
- Intersecting rings: A topology in which two ERPS rings share two devices is called intersecting rings. Major ring ERPS 4 (node 13-10-11-12) and subring ERPS 5 (node 13-15-14-12) constitute an intersecting-ring topology, and intersect on two directly connected intersecting nodes, namely, node 13 and node 12.

In practice, a network is a combination of multiple basic topologies, with multiple major rings and multiple subrings.

3. Node

According to the different topological relationships between nodes and Ethernet rings, nodes are classified into single-ring nodes, tangent nodes, and intersecting nodes by role.

- Single-ring node: In an Ethernet ring, the nodes that belong to only one Ethernet ring (either major ring or subring) are called single-ring nodes. Two physical ports need to be provided on a single-ring node so that the node can be added to one ERPS ring. As shown in Figure 1-1, nodes 1-4 in the single-ring topology, nodes 5, 6, 8, and 9 in the tangent-ring topology, and nodes 10, 11, 14, and 15 in the intersecting-ring topology are all single-ring nodes.
- Tangent node: A device shared in tangent rings is called a tangent node. Four physical ports need to be provided on each tangent node, with two added to a major ring and the other two added to another major ring. As shown in Figure 1-1, node 7 in the tangent-ring topology is a tangent node.
- Intersecting node: The nodes in intersecting rings that belong to multiple rings are called intersecting nodes. The intersecting nodes must be connected directly without any other nodes in between. Three physical ports need to be provided on a tangent node, with two added to a major ring and the other added to a subring. As shown in Figure 1-1, nodes 12 and 13 in the intersecting-ring topology are intersecting nodes. ERPS rings can intersect with other multiple ERPS rings and share links to implement data link redundancy. Services can be quickly switched from a failed link in one ERPS ring to a normal link.

4. Ring Member Port

An Ethernet ring has two ring member ports on each node that it passes through: the **west** and **east** ports. As shown in Figure 1-1:

- If an ERPS ring is a closed major ring, each node that the ring passes through has two physical ports used as the **west** and **east** ports for adding the node to the ERPS ring. For example, on node 7, GigabitEthernet 0/1 and 0/2 are added to the major ring ERPS 2, and GigabitEthernet 0/3 and 0/4 are added to the major ring ERPS 3. On node 13, GigabitEthernet 0/5 and 0/6 are added to the major ring ERPS 4.
- If an ERPS ring is a non-closed subring (in an intersecting-ring topology), a non-intersecting node has two physical ports used as the **west** and **east** ports for adding the node to the ERPS subring, such as node 15. On an intersecting node, only one physical port is added to the ERPS subring as a ring member port, and the other ring member port is a virtual channel (indicated by **virtual-channel**). For example, on node 13, only GigabitEthernet 0/7 is added to the subring ERPS 5.

There are two states for a port running the ERPS protocol: forwarding and discarding. Their functions are listed in Table 1-1.

Table 1-1 ERPS Protocol Port States

Port State	Receiving Protocol Packets	Sending Protocol Packets	Address Learning	Receiving Data Packets	Sending Data Packets
Discarding	Yes	Yes	No	No	No
Forwarding	Yes	Yes	Yes	Yes	Yes

1.1.4 RPL and Nodes

An Ethernet ring can be in either of the following two states regardless of whether it is a major ring or subring:

- Idle state: The physical links in the entire ring network are connected.
- Protection state: A physical link in the ring network is disconnected.

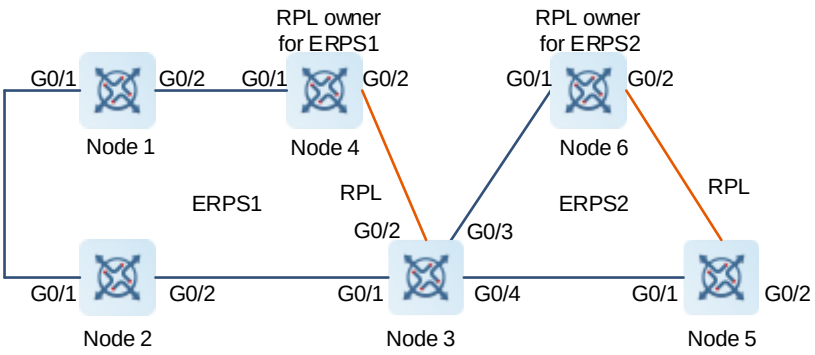
Ring protection link (RPL): When the physical links in a ring network are connected, the ERPS ring is in the idle state, and the links in the logic blocking state are RPLs. Each Ethernet ring has only one RPL. For example, the links indicated by the orange lines shown in Figure 1-2 are RPLs, the link between node 3 and node 4 is the RPL of the Ethernet ring ERPS 1 (node 1-2-3-4), and the link between node 5 and node 6 is the RPL of the Ethernet ring ERPS 2 (node 3-5-6).

A node that is adjacent to an RPL and is used to block the RPL to prevent loops when the Ethernet ring is free of faults is called an RPL owner node. As shown in Figure 1-2, node 4 is the RPL owner node of the Ethernet ring ERPS 1 (node 1-2-3-4) and node 6 is the RPL owner node of the ERPS 2 (node 3-5-6).

Any nodes other than the RPL owner node in an Ethernet ring are non-RPL owner nodes. As shown in Figure 1-2, nodes except node 4 and node 6 are non-RPL owner nodes of the rings.

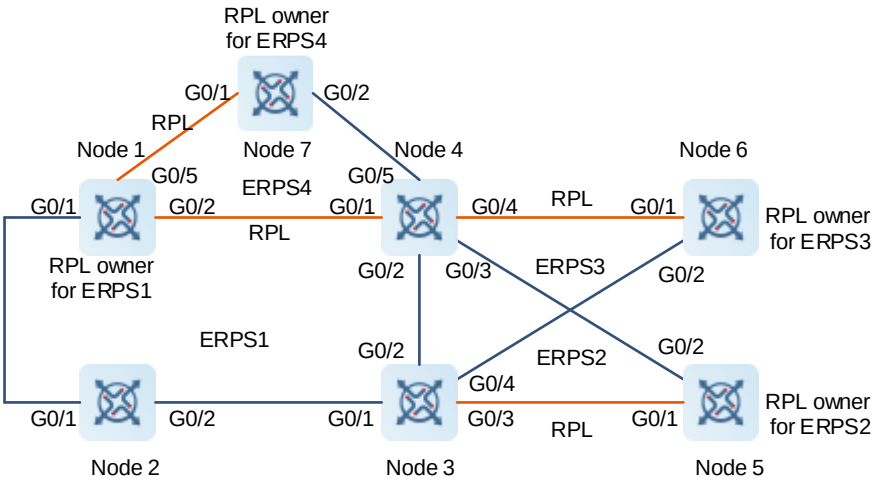
Blocked ports on RPLs are RPL ports, and RPL ports do not forward data packets to prevent loops. RPL ports are on RPL owner nodes, and the RPL owner nodes block the RPL ports. Each Ethernet ring has only one RPL owner node.

Figure 1-2 Typical Topology of Tangent Rings



As shown in Figure 1-2, the link between node 3 and node 4 is the RPL of the Ethernet ring ERPS 1. As the RPL owner node of ERPS 1, node 4 blocks the RPL port. The link between node 5 and node 6 is the RPL of the Ethernet ring ERPS 2. As the RPL owner node of ERPS 2, node 6 blocks the RPL port. ERPS 1 (node 1-2-3-4) and ERPS 2 (node 3-5-6) share node 3, forming a tangent-ring topology. Node 3 is the tangent node.

Figure 1-3 Typical Topology of Intersecting Rings



As shown in Figure 1-3, ERPS 1 (node 1-2-3-4) is a major ring, and ERPS 2 (node 3-4-5) is a subring. ERPS 1 and ERPS 2 share node 3 and node 4, forming an intersecting-ring topology. The links between node 4 and node 5, and between node 3 and node 5 are links of the subring ERPS 2 and are controlled by ERPS 2. The link between node 3 and node 4 belongs to the major ring not the subring, and is not controlled by the subring. However, the protocol packets of the subring are transmitted through the direct link between node 3 and node 4. This direct link is the R-APS virtual channel of the subring ERPS 2. Node 2 only belongs to the major ring ERPS 1, and is called a single-ring node. Node 6 only belongs to the subring ERPS 3, and is also called a single-ring node. Node 3 and node 4 are tangent nodes.

1.1.5 ERPS Packet

ERPS packets (also called R-APS packets) are classified into Signal Fail (SF) packets, No Request (NR) packets, No Requests-RPL Blocked (NR-RB) packets, and Flush packets.

- SF packet: When the link of a node is down, the node sends an SF packet to notify other nodes of its link

failure.

- NR packet: When the failed link is restored, the node sends an NR packet to notify the RPL owner node of its link recovery.
- NR-RB packet: When all nodes in an ERPS ring function properly, the RPL owner node sends NR-RB packets periodically.
- Flush packet: In intersecting rings, when a topology change occurs in a subring, the intersecting nodes send flush packets to notify other devices in the Ethernet ring to which the subring is connected.

1.1.6 ERPS Timer

ERPS supports three timers: Holdoff timer, Guard timer, and Wait-To-Restore (WTR) timer.

- Holdoff timer: The timer is used to minimize frequent ERPS topology switching due to intermittent link failures. After you configure the Holdoff timer, ERPS performs topology switching only if the link failure still persists after the timer times out.
- Guard timer: The timer is used to prevent a device from receiving expired R-APS PMDU packets. When a device detects that a link failure is cleared, it sends link recovery packets and starts the Guard timer. Before the timer expires, all packets except Flush packets indicating a subring topology change will be discarded.
- WTR timer: The timer is effective only for RPL owner nodes. It is used to avoid ring status misjudgment by the RPL owner node. When an RPL owner node detects that a failure is cleared, it will not perform topology switching immediately but only if the Ethernet ring is recovered after the WTR timer times out. If a ring failure is detected again before the timer expires, the RPL owner node cancels the timer and does not perform topology switching.

1.1.7 Ring Protection

The ring protection function prevents broadcast storms caused by data loops and can rapidly recover the communication between nodes when a link is disconnected in the Ethernet ring.

- Normal state
  - All nodes in the physical topology are connected in ring mode.
  - ERPS blocks the RPL to prevent loops.
  - ERPS detects failures on each link between adjacent nodes.
- Link fault
  - A node adjacent to a failed node detects the fault.
  - The node adjacent to the failed link blocks the failed link and sends SF packets to notify other nodes in the same ring.
  - An SF packet triggers the RPL owner node to enable the RPL port, and also triggers all nodes to update their MAC address entries and ARP/ND entries and enter the protection state.
- Link recovery
  - When a failed link is restored, an adjacent node still blocks the link and sends NR packets indicating that no local fault exists.
  - When the RPL owner node receives the first NR packet, it starts the WTR timer.
  - When the WTR timer times out, the RPL owner node blocks the RPL and sends an NR-RB packet.

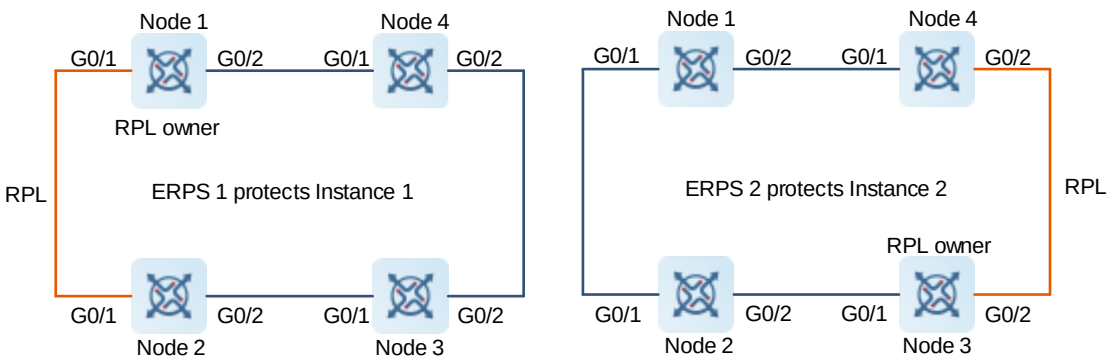
- After receiving this NR-RB packet, other nodes update their MAC address entries and ARP/ND entries, and the node that sends the NR packet stops sending the NR packet and enables the blocked ports.
- The ring network is restored to the normal state.

1.1.8 Load Balancing

One control VLAN identifies one ERPS ring and corresponds to the data VLANs that it needs to protect. By default, an ERPS ring protects all VLANs. You do not need to configure the VLANs to be protected by an Ethernet ring.

If multiple control VLANs are configured in the same physical ring network to form multiple Ethernet rings and they need to protect different data VLANs, load balancing can be achieved. In this case, the traffic from different VLANs is forwarded along their respective paths. When a link in the ring network with load balancing enabled fails, the traffic can be quickly switched to a normal link.

Figure 1-4 Typical Application of Load Balancing



As shown in Figure 1-4, two Ethernet rings (ERPS 1 and ERPS 2) are configured on the physical ring network to protect different VLANs. Node 1 is the RPL owner of ERPS 1, and node 3 is the RPL owner of ERPS 2. With such configurations, data of different VLANs can be transmitted by different links to achieve load balancing.

1.1.9 Protocols and Standards

ITU-T G.8032/Y.1344: Ethernet ring protection switching

1.2 Configuration Task Summary

The configuration includes the following tasks:

(1) Configuring a Control VLAN for an Ethernet Ring

(2) Configuring Member Ports for an Ethernet Ring

(3) (Optional) Configuring an RPL Port

(4) (Optional) Configuring Major Rings to Associate with Subrings

(5) (Optional) Configuring Subring Topology Change Notification

(6) (Optional) Configuring a Protected VLAN for an Ethernet Ring

(7) Enabling ERPS for an Ethernet Ring

(8) (Optional) Configuring ERPS Timers

(9) Enabling ERPS Globally

1.3 Configuring a Control VLAN for an Ethernet Ring

1.3.1 Overview

A control VLAN, also known as an R-APS VLAN, is used to transmit ERPS protocol packets. A group of interconnected devices in the same control VLAN constitute an Ethernet ring (ERPS ring). For an ERPS ring, the same Ethernet ring R-APS VLAN needs to be configured on each node that it passes through. In practice, one or more ERPS rings may pass through a node, and one control VLAN needs to be configured for each ERPS ring on the node.

- As shown in Figure 1-2, ERPS 1 (node 1-2-3-4) is tangent to ERPS 2 (node 3-5-6) on node 3, on which two ERPS control VLANs need to be created.
- As shown in Figure 1-3, the major ring ERPS 1 (node 1-2-3-4) intersects the subring ERPS 2 (node 3-4-5) on node 3, and the major ring ERPS 1 (node 1-2-3-4) also intersects the subring ERPS 3 (node 3-4-6) on node 3, on which three ERPS control VLANs need to be created.
- As shown in Figure 1-3, only the major ring ERPS 1 (node1-2-3-4) passes through node 2, on which only one ERPS control VLAN needs to be created. Only the subring ERPS 2 (node 3-4-5) passes through node 5, on which only one ERPS control VLAN needs to be created.

1.3.2 Restrictions and Guidelines

- An R-APS VLAN must be an unused VLAN on a device. VLAN 1 cannot be configured as an R-APS VLAN.
- The packets of different ERPS rings are distinguished using the control VLANs (R-APS VLANs). Therefore, the control VLANs of different ERPS rings must be different.
- If a device with ERPS disabled needs to transparently transmit ERPS packets, ensure that only the two ports connecting the device to an ERPS ring allow packets from the control VLAN of the ERPS ring to pass through. Otherwise, packets from other VLANs may be transparently transmitted to the R-APS VLAN, causing impact on the ERPS ring.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a control VLAN for an Ethernet ring.

erps raps-vlan *vlan-id*

No R-APS VLAN is configured by default.

1.4 Configuring Member Ports for an Ethernet Ring

1.4.1 Overview

An Ethernet ring has two ring member ports on each node that it passes through: the **west** and **east** ports.

If an ERPS ring is a closed major ring, each node that the ring passes through has two physical ports used as the **west** and **east** ports for adding the node to the ERPS ring. If an ERPS ring is a non-closed subring, a non-intersecting node has two physical ports used as the **west** and **east** ports for adding the node to the ERPS subring. On an intersecting node, only one physical port is added to the ERPS subring as a ring member port, and the other ring member port is a virtual channel (indicated by **virtual channel**).

According to the type of an ERPS ring (major ring or subring), add a physical port or virtual channel of a node to the control VLAN of an ERPS ring so that the port becomes a member port.

1.4.2 Restrictions and Guidelines

- If an Ethernet ring (major or subring) passes through two physical ports on a node, run the **ring-port west** *interface-type interface-number-1* **east** *interface-type interface-number-2* command to add the two physical ports to the Ethernet ring.
- If an Ethernet ring (subring only) passes through one physical port on a node, run the **ring-port west** *interface-type interface-number* **east virtual-channel** command to configure the physical port as the west port of the Ethernet ring, or run the **ring-port west virtual-channel east** *interface-type interface-number* command to configure the physical port as the east port of the Ethernet ring.
- Only trunk ports can be added to an ERPS ring. The trunk attributes of a port cannot be modified after it is added to an ERPS ring. To modify the trunk attributes, enter the control VLAN configuration mode (that is, R-APS VLAN configuration mode), and run the **no ring-port** command to delete the port from the ERPS ring.
- The ports added to an ERPS ring will not participate in the spanning tree calculation no matter whether the ERPS ring is enabled. When you configure an ERPS ring, ensure that loops do not exist on the member ports of the ring.
- In R-APS VLAN configuration mode, configure the ports that form an ERPS ring as ERPS ring ports.
- ERPS cannot share ports with the Rapid Ethernet Ring Protection (RERP) and Rapid Ethernet Uplink Protection (REUP).
- Do not configure IP address on the ring member ports; otherwise ERPS may be abnormal.
- When an ERPS ring topology changes and a port needs to be modified, to avoid loops during configuration modification, do as follows in sequence: Run the **shutdown** command to shut down one ERPS port in this ring. Enter the control VLAN configuration mode and run the **no state enable** command to disable the ERPS function. Run the **no ring-port** command to delete the ring member port. Finally, add a new member port to the Ethernet ring and run the **state enable** command to enable the ERPS function for the Ethernet ring. Upon completion of configuration, run the **no shutdown** command to enable the port.

1.4.3 Procedure

(1) Configure physical ports as trunk ports.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Enter the interface configuration mode of the ring member ports.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

d Set the links of the ring member ports to work in trunk mode.

switchport mode trunk

An interface link works in access mode by default.

e Return to the global configuration mode.

exit

(2) Enter the R-APS VLAN configuration mode of an Ethernet ring.

erps raps-vlan *vlan-id*

(3) Configure the member ports for the Ethernet ring.

ring-port west { *interface-type interface-number* | **virtual-channel** } **east** { *interface-type interface-number* | **virtual-channel** }

No member port exists in an ERPS ring by default.

1.5 Configuring an RPL Port

1.5.1 Overview

Each ERPS ring has only one RPL and only one RPL owner node. Blocked ports on RPLs are RPL ports, which do not forward data packets to prevent loops.

On an ERPS ring, select a device as the RPL owner, enter the R-APS VLAN configuration mode of the Ethernet ring on this device, and configure the west or east port as an RPL port. For non-RPL owner nodes, no RPL port needs to be configured.

1.5.2 Restrictions and Guidelines

- The **west** parameter indicates that the west port is specified as an RPL port, and the **east** parameter indicates that the east port is specified as an RPL port.
- Two tangent rings have two RPLs and two RPL owner nodes. However, do not configure a tangent node as an RPL owner node.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the R-APS VLAN configuration mode of an Ethernet ring.

erps raps-vlan *vlan-id*

(4) Configure an RPL port on an RPL owner node.

rpl-port { **west** | **east** } **rpl-owner**

No RPL port exists in an ERPS ring by default.

1.6 Configuring Major Rings to Associate with Subrings

1.6.1 Overview

When there are intersecting rings in an Ethernet ring topology, the major ring needs to be configured to associate with all subrings on all nodes in the major ring (no matter whether the subrings are directly connected to the nodes) so that the ERPS packets of subrings can be transmitted in the major ring. The association of major rings with subrings does not need to be configured on nodes only in subrings.

1.6.2 Restrictions and Guidelines

- On all nodes in a major ring of intersecting rings, including intersecting nodes and non-intersecting nodes, the association of the major ring with all subrings needs to be configured so that the ERPS packets of the subrings can be transmitted in the major ring.
- You can also use the command provided by the VLAN module to configure a control VLAN and its member ports so that ERPS packets of subrings can be transmitted in other Ethernet rings and are not leaked to user networks.
- If the subring topology change notification has been configured in a subring of intersecting rings and the link between intersecting nodes is faulty or blocked in the event of a subring topology change, the intersecting nodes will send packets to instruct the nodes in other Ethernet rings associated with the subring to update the topology.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the control VLAN configuration mode of a major ring.

erps raps-vlan *vlan-id*

(4) Associate the major ring with all subrings.

associate sub-ring raps-vlan *vlan-list*

An ERPS major ring is not associated with any subrings by default.

1.7 Configuring Subring Topology Change Notification

1.7.1 Overview

This function is required only in the subrings on intersecting nodes. When the subring topology changes, the intersecting nodes send a topology change notification.

1.7.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the control VLAN configuration mode of a subring.

erps raps-vlan *vlan-id*

(4) Enable the subring topology change notification.

sub-ring tc-propagation enable

1.8 Configuring a Protected VLAN for an Ethernet Ring

1.8.1 Overview

This section describes how to configure the data VLANs to be protected by an ERPS ring. All VLANs are protected by an ERPS ring by default. When load balancing is needed, multiple Ethernet rings can be configured on the same physical ring network, and different Ethernet rings protect different VLANs. In this way, different Ethernet rings send traffic from different VLANs separately, achieving load balancing. When a link in a ring network with load balancing enabled fails, the traffic can be quickly switched to a normal link.

1.8.2 Restrictions and Guidelines

- Before you configure load balancing, configure the mapping between VLANs and instances in MST configuration mode.
- When you configure load balancing, add all data VLANs of the devices to the ERPS protected VLAN list; otherwise, any unprotected VLAN may cause loops.
- Configure protected VLANs for an Ethernet ring in global configuration mode after you complete the single-ring configuration.

1.8.3 Procedure

(1) Configure the mapping between instances and VLANs.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Enter the MST configuration mode.

spanning-tree mst configuration

d Add a VLAN group to an MST instance.

instance *instance-id* **vlan** *vlan-range*

e Return to the global configuration mode.

exit

(2) Enter the control VLAN configuration mode of an Ethernet ring.

erps raps-vlan *vlan-id*

(3) Configure the Ethernet ring to protect the defined instance so as to protect the specified data VLANs.

protected-instance *instance-id-list*

An Ethernet ring protects all VLANs by default.

1.9 Enabling ERPS for an Ethernet Ring

1.9.1 Overview

This section describes how to enter the R-APS VLAN configuration mode of a specified Ethernet ring, and enable the ERPS function for this Ethernet ring. If more than one Ethernet ring passes through a node, the ERPS function of each Ethernet ring needs to be enabled separately.

1.9.2 Restrictions and Guidelines

ERPS takes effect only after ERPS is enabled both globally and for a specified ring on each node that the Ethernet ring passes through.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the R-APS VLAN configuration mode of an Ethernet ring.

erps raps-vlan *vlan-id*

No R-APS VLAN is configured by default.

(4) Enable the ERPS function of the Ethernet ring.

state enable

The ERPS function of an Ethernet ring is disabled by default.

1.10 Configuring ERPS Timers

1.10.1 Overview

This section describes how to configure the Holdoff, Guard, and WTR timers.

1.10.2 Restrictions and Guidelines

- Run the **timer holdoff-time** command to configure the Holdoff timer. *interval1* indicates the value of the Holdoff timer, in 100 milliseconds. The value range is from 0 to 100, and the default value is **0**.
- Run the **timer guard-time** command to configure the Guard timer. *interval2* indicates the value of the Guard timer, in 10 milliseconds. The value range is from 1 to 200, and the default value is **50**.
- Run the **timer wtr-time** command to configure the WTR timer. *interval3* indicates the value of the WTR timer, in minutes. The value range is from 1 to 12, and the default value is **2**.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the control VLAN configuration mode.

erps raps-vlan *vlan-id*

(4) Configure a timer.

timer { **holdoff-time** *interval1* | **guard-time** *interval2* | **wtr-time** *interval3* }

1.11 Enabling ERPS Globally

1.11.1 Overview

After completing all configurations of the ERPS function, you need to enable ERPS globally on each node that an Ethernet ring passes through so that ERPS takes effect.

1.11.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the global ERPS function.

erps enable

The global ERPS function is disabled by default.

1.12 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** commands to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

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

Table 1-2 Monitoring

Command	Purpose
show erps [**global** | **raps_vlan** *vlan-id* [*sub_ring*]]	Displays the ERPS configuration and state of a device.

1.13 Configuration Examples

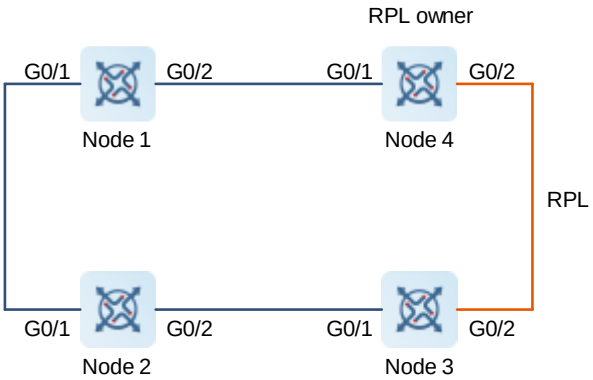
1.13.1 Configuring Single-Ring Protection

1. Requirements

As shown in Figure 1-5, there is only one ring in the network topology. All nodes are connected in a ring in the physical topology. ERPS blocks the RPL to prevent loops, and detects faults on each link between adjacent nodes. There is only one RPL owner node and only one RPL in an Ethernet ring. All nodes must belong to the same R-APS VLAN. All devices in the ring network must support ERPS. Each link between devices must be a direct link without any intermediate device.

2. Topology

Figure 1-5 Application Scenario of Single-Ring Protection



3. Notes

- Before adding a physical port to an Ethernet ring, configure the link of the member port to work in trunk mode.
- Node 1, node 2, and node 3 are all non-RPL owner nodes, through which only ERPS 1 passes. Notes for configuring these nodes are as follows:
  - Configure R-APS VLAN 100, add physical ports GigabitEthernet 0/1 and 0/2 to the Ethernet ring, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.
- Only ERPS 1 passes through node 4 and node 4 is the RPL owner node of the ERPS ring. Notes for configuring this node are as follows:
  - Configure R-APS VLAN 100, add physical ports GigabitEthernet 0/1 and 0/2 to the Ethernet ring, configure GigabitEthernet 0/2 as an RPL port, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.

4. Procedure

(1) Configure single-ring nodes (node 1, node 2, and node 3) in the same way. The following uses node 1 as an example.

Configure the links of the member ports to work in trunk mode.

```
Node1> enable
Node1# configure terminal
Node1(config)# interface range gigabitethernet 0/1-2
Node1(config-if-rang)# switchport
Node1(config-if-rang)# switchport mode trunk
Node1(config-if-rang)# exit
```

Create an Ethernet ring control VLAN, that is, R-APS VLAN 100.

```
Node1(config)# erps raps-vlan 100
```

Add the two physical ports GigabitEthernet 0/1 and 0/2 to the Ethernet ring.

```
Node1(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
```

Enable the ERPS function for the Ethernet ring.

```
Node1(config-erps 100)# state enable
Node1(config-erps 100)# exit
```

Enable the global ERPS function.

```
Node1(config)# erps enable
```

(2) Configure node 4 that is a single-ring node and an RPL owner node.

Configure the links of the member ports to work in trunk mode.

```
Node4> enable
Node4# configure terminal
Node4(config)# interface range gigabitethernet 0/1-2
Node1(config-if-rang)# switchport
Node4(config-if-range)# switchport mode trunk
Node4(config-if-range)# exit
```

Create an Ethernet ring control VLAN, that is, R-APS VLAN 100.

```
Node4(config)# erps raps-vlan 100
```

Add the two physical ports GigabitEthernet 0/1 and 0/2 to the Ethernet ring.

```
Node4(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
```

Configure GigabitEthernet 0/2 (east) as the RPL port of R-APS VLAN 100.

```
Node4(config-erps 100)# rpl-port east rpl-Owner
```

Enable the ERPS function for the Ethernet ring.

```
Node4(config-erps 100)# state enable
Node4(config-erps 100)# exit
```

Enable the global ERPS function.

```
Node4(config)# erps enable
```

5. Verification

(1) Verify the configurations of non-RPL owner nodes: node 1, node 2, and node 3. These three nodes use the same configurations. The following uses node 1 as an example.

```
Node1# show erps
```

```
ERPS Information
Global Status             : Enabled
Link monitored by          : Not Oam
-------------------------------------------
R-APS VLAN                : 100
Ring Status               : Enabled
West Port                 : Gi0/1       (Forwarding)
East Port                 : Gi0/2       (Forwarding)
RPL Port                  : None
Protected VLANs            : ALL
RPL Owner                 : Disabled
Holdoff Time               : 0 milliseconds
Guard Time                : 500 milliseconds
WTR Time                  : 2 minutes
Current Ring State         : idle
Associate R-APS VLAN        :
```

(2) Verify the configurations of node 4, an RPL owner node.

```
Node4# show erps
ERPS Information
Global Status             : Enabled
Link monitored by          : Not Oam
-------------------------------------------
R-APS VLAN                : 100
Ring Status               : Enabled
West Port                 : Gi0/1       (Forwarding)
East Port                 : Gi0/2       (Blocking)
RPL Port                  : East Port
Protected VLANs            : ALL
RPL Owner                 : Enabled
Holdoff Time               : 0 milliseconds
Guard Time                : 500 milliseconds
WTR Time                  : 2 minutes
Current Ring State         : idle
Associate R-APS VLAN        :
```

6. Configuration Files

- Configuration files for node 1, node 2, and node 3

```
erps enable
!
erps raps-vlan 100
 ring-port west GigabitEthernet 0/1 east GigabitEthernet 0/2
 state enable
!
interface GigabitEthernet 0/1
 switchport mode trunk
```

```
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

- Configuration file for node 4

```
erps enable
!
erps raps-vlan 100
 ring-port west GigabitEthernet 0/1 east GigabitEthernet 0/2
 rpl-port east rpl-Owner
 state enable
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

7. Common Errors

- Different R-APS VLANs are configured for the nodes in one ring.
- The ERPS function is not enabled globally and for an Ethernet ring on all nodes in the Ethernet ring. As a result, the ERPS function does not take effect.
- Multiple RPL owner nodes are configured in one ring.
- If member ports on an RPL owner node in an Ethernet ring are modified, the configuration of the RPL port will be deleted by the system. The RPL owner node may fail to operate properly if the RPL port is not configured again.

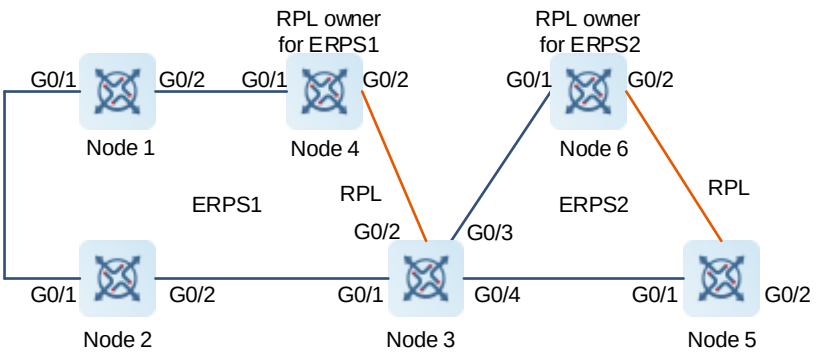
1.13.2 Configuring Tangent-Ring Protection

1. Requirements

In the network topology shown in Figure 1-6, two ring networks share the same device to implement ERPS protection. ERPS is used to detect faults on each link between adjacent nodes. All nodes are connected in a ring in a physical topology. ERPS blocks the RPL of each ring to prevent loops. Each ring has only one RPL owner node and only one RPL. Different rings belong to different R-APS VLANs. All devices in the ring network must support ERPS. Each link between devices must be a direct link without any intermediate device.

2. Topology

Figure 1-6 Application Scenario of Tangent-Ring Protection



3. Notes

- Before adding a physical port to an Ethernet ring, configure the link of the member port to work in trunk mode.
- Node 1 and node 2 are non-RPL owner nodes, through which only ERPS 1 passes. Notes for configuring these nodes are as follows:
  - Configure R-APS VLAN 100, add GigabitEthernet 0/1 and 0/2 to the Ethernet ring, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.
- Node 3 is the tangent node of ERPS 1 and ERPS 2. Notes for configuring this node are as follows:
  - Configure R-APS VLAN 100, add GigabitEthernet 0/1 and 0/2 to R-APS VLAN 100, and enable the ERPS function for the Ethernet ring.
  - Configure R-APS VLAN 200, add GigabitEthernet 0/3 and 0/4 to R-APS VLAN 200, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.
- Only ERPS 1 passes through node 4 and node 4 is the RPL owner node of ERPS 1. Notes for configuring this node are as follows:
  - Configure R-APS VLAN 100, add GigabitEthernet 0/1 and 0/2 to the Ethernet ring, configure GigabitEthernet 0/2 as an RPL port, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.
- Only ERPS 2 passes through node 5 and node 5 is a non-RPL owner node. Notes for configuring this node are as follows:
  - Configure R-APS VLAN 200, add GigabitEthernet 0/1 and 0/2 to the Ethernet ring, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.
- Only ERPS 2 passes through node 6 and node 6 is the RPL owner node of ERPS 2. Notes for configuring this node are as follows:
  - Configure R-APS VLAN 200, add GigabitEthernet 0/1 and 0/2 to the Ethernet ring, configure

GigabitEthernet 0/2 as an RPL port, and enable the ERPS function for the Ethernet ring.

- Enable the global ERPS function.

4. Procedure

(1) Configure single-ring nodes (node 1 and node 2) of ERPS 1 in the same way. The following uses node 1 as an example.

Configure the links of Ethernet ring ports GigabitEthernet 0/1 and 0/2 of ERPS 1 to work in trunk mode. Create the Ethernet ring R-APS VLAN 100, add physical ports to the Ethernet ring, and enable the ERPS function for the Ethernet ring.

```
Node1> enable
Node1# configure terminal
Node1(config)# interface range gigabitethernet 0/1-2
Node1(config-if-range)# switchport mode trunk
Node1(config-if-range)# exit
Node1(config)# erps raps-vlan 100
Node1(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node1(config-erps 100)# state enable
Node1(config-erps 100)# exit
```

Enable the global ERPS function.

```
Node1(config)# erps enable
```

(2) Configure the tangent node: node 3.

Configure the links of Ethernet ring ports GigabitEthernet 0/1 and 0/2 of ERPS 1 to work in trunk mode. Create the Ethernet ring R-APS VLAN 100, add physical ports to the Ethernet ring, and enable the ERPS function for the Ethernet ring.

```
Node3> enable
Node3# configure terminal
Node3(config)# interface range gigabitethernet 0/1-2
Node3(config-if-range)# switchport mode trunk
Node3(config-if-range)# exit
Node3(config)# erps raps-vlan 100
Node3(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node3(config-erps 100)# state enable
Node3(config-erps 100)# exit
```

Configure the links of Ethernet ring ports GigabitEthernet 0/3 and GigabitEthernet 0/4 of ERPS 2 to work in trunk mode. Create the Ethernet ring R-APS VLAN 200, add physical ports to the Ethernet ring, and enable the ERPS function for the Ethernet ring.

```
Node3(config)# interface range gigabitethernet 0/3-4
Node3(config-if-range)# switchport mode trunk
Node3(config-if-range)# exit
Node3(config)# erps raps-vlan 200
```

```
Node3(config-erps 200)# ring-port west gigabitethernet 0/3 east gigabitethernet
0/4
Node3(config-erps 200)# state enable
Node3(config-erps 200)# exit
```

Enable the global ERPS function.

```
Node3(config)# erps enable
```

(3) Configure node 4 that is a single-ring node and an RPL owner node of ERPS 1.

Configure the links of Ethernet ring ports GigabitEthernet 0/1 and 0/2 of ERPS 1 to work in trunk mode. Create Ethernet ring R-APS VLAN 100 and add physical ports to the Ethernet ring. Specify the RPL owner port and enable the ERPS function for the Ethernet ring.

```
Node4> enable
Node4# configure terminal
Node4(config)# interface gigabitethernet 0/1
Node4(config-if-GigabitEthernet 0/1)# switchport mode trunk
Node4(config-if-GigabitEthernet 0/1)# exit
Node4(config)# interface gigabitethernet 0/2
Node4(config-if-GigabitEthernet 0/2)# switchport mode trunk
Node4(config-if-GigabitEthernet 0/2)# exit
Node4(config)# erps raps-vlan 100
Node4(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node4(config-erps 100)# rpl-port east rpl-owner
Node4(config-erps 100)# state enable
Node4(config-erps 100)# exit
```

Enable the global ERPS function.

```
Node4(config)# erps enable
```

(4) Configure the single-ring node (node 5) of ERPS 2.

Configure the links of Ethernet ring ports GigabitEthernet 0/1 and GigabitEthernet 0/2 of ERPS 2 to work in trunk mode. Create Ethernet ring R-APS VLAN 200, add physical ports to the Ethernet ring, and enable the ERPS function for the Ethernet ring.

```
Node5> enable
Node5# configure terminal
Node5(config)# interface gigabitethernet 0/1
Node5(config-if-GigabitEthernet 0/1)# switchport mode trunk
Node5(config-if-GigabitEthernet 0/1)# exit
Node5(config)# interface gigabitethernet 0/2
Node5(config-if-GigabitEthernet 0/2)# switchport mode trunk
Node5(config-if-GigabitEthernet 0/2)# exit
Node5(config)# erps raps-vlan 200
Node5(config-erps 200)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node5(config-erps 200)# state enable
Node5(config-erps 200)# exit
```

Enable the global ERPS function.

```
Node5(config)# erps enable
```

(5) Configure node 6 that is a single-ring node and an RPL owner node of ERPS 2.

Configure the links of Ethernet ring ports GigabitEthernet 0/1 and GigabitEthernet 0/2 of ERPS 2 to work in trunk mode. Create Ethernet ring R-APS VLAN 200 and add physical ports to the Ethernet ring. Specify the RPL owner port and enable the ERPS function for the Ethernet ring.

```
Node6> enable
Node6# configure terminal
Node6(config)# interface gigabitethernet 0/1
Node6(config-if-GigabitEthernet 0/1)# switchport mode trunk
Node6(config-if-GigabitEthernet 0/1)# exit
Node6(config)# interface gigabitethernet 0/2
Node6(config-if-GigabitEthernet 0/2)# switchport mode trunk
Node6(config-if-GigabitEthernet 0/2)# exit
Node6(config)# erps raps-vlan 100
Node6(config-erps 200)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node6(config-erps 200)# rpl-port east rpl-owner
Node6(config-erps 200)# state enable
```

Enable the global ERPS function.

```
Node6(config)# erps enable
```

5. Verification

Run the **show erps** command on each node to verify the configuration. The following uses node 3 as an example.

```
Node3# show erps
ERPS Information
Global Status                 : Enabled
Link monitored by             : Not Oam
--------------------------------------------
R-APS VLAN                    : 200
Ring Status                   : Enabled
West Port                     : Gi 0/3 (Forwarding)
East Port                     : Gi 0/4 (Forwarding)
RPL Port                      : None
Protected VLANs               : ALL
RPL Owner                     : Disabled
Holdoff Time                  : 0 milliseconds
Guard Time                    : 500 milliseconds
WTR Time                      : 2 minutes
Current Ring State            : Idle
Associate R-APS VLAN          :
--------------------------------------------
R-APS VLAN                    : 100
Ring Status                   : Enabled
West Port                     : Gi 0/1 (Forwarding)
```

```
East Port                       : Gi 0/2 (Forwarding)
RPL Port                        : East Port
Protected VLANs                 : ALL
RPL Owner                       : Disabled
Holdoff Time                    : 0 milliseconds
Guard Time                      : 500 milliseconds
WTR Time                        : 2 minutes
Current Ring State              : Idle
Associate R-APS VLAN            :
```

6. Common Errors

- An R-APS ring has been enabled but ERPS is not enabled globally, so ERPS does not take effect yet.
- Multiple RPL owner nodes are configured in one ring.
- Different R-APS VLANs are configured for the nodes in one ring.

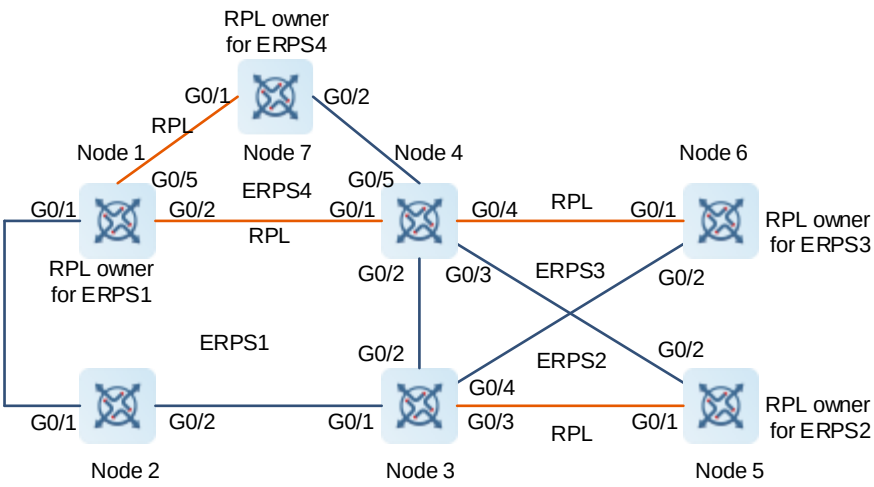
1.13.3 Configuring Intersecting-Ring Protection

1. Requirements

As shown in Figure 1-7, there are four rings in the network topology. All nodes are connected in a ring in the physical topology. Nodes are connected through direct links. Each ring has only one RPL owner node and only one RPL. Two or more rings share one link. All devices in the ring network support ERPS. Configure ERPS. ERPS blocks the RPL of each ring to prevent loops, and detects faults on each link between adjacent nodes.

2. Topology

Figure 1-7 Application Scenario of Intersecting-Ring Protection



3. Notes

- Before adding a physical port to an Ethernet ring, configure the link of the member port to work in trunk mode.
- Node 1 is the intersecting node of the major ring ERPS 1 and subring ERPS 4, as well as the RPL owner node of ERPS 1. Notes for configuring this node are as follows:

- Configure R-APS VLAN 100, add GigabitEthernet 0/1 and GigabitEthernet 0/2 to R-APS VLAN 100, configure GigabitEthernet 0/2 as the RPL port, associate the major ring with subrings R-APS VLANs 200, 300, and 400, and enable the ERPS function for the Ethernet ring.
- Configure subring R-APS VLAN 400, add GigabitEthernet 0/5 and virtual channel to R-APS VLAN 400, and enable the ERPS function for the Ethernet ring.
- Enable the global ERPS function.

- Only major ring ERPS 1 passes through node 2. Notes for configuring this node are as follows:
  - Configure R-APS VLAN 100, add GigabitEthernet 0/1 and GigabitEthernet 0/2 to R-APS VLAN 100, associate the major ring with subrings R-APS VLANs 200, 300, and 400, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.
- Node 3 is the intersecting node of the major ring ERPS 1 and subrings ERPS 2 and ERPS 3. Notes for configuring this node are as follows:
  - Configure the major ring R-APS VLAN 100, add GigabitEthernet 0/1 and GigabitEthernet 0/2 to R-APS VLAN 100, associate the major ring with subrings R-APS VLANs 200, 300, and 400, and enable the ERPS function for the Ethernet ring.
  - Configure subring R-APS VLAN 200, add GigabitEthernet 0/3 and virtual channel to R-APS VLAN 200, and enable the ERPS function for the Ethernet ring.
  - Configure subring R-APS VLAN 300, add GigabitEthernet 0/4 and virtual channel to R-APS VLAN 300, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.
- Node 4 is the intersecting node of the major ring ERPS 1 and subrings ERPS 2, ERPS 3, and ERPS4. Notes for configuring this node are as follows:
  - Configure the major ring R-APS VLAN 100, add GigabitEthernet 0/1 and GigabitEthernet 0/2 to R-APS VLAN 100, associate the major ring with subrings R-APS VLANs 200, 300, and 400, and enable the ERPS function for the Ethernet ring.
  - Configure subring R-APS VLAN 200, add GigabitEthernet 0/3 and virtual channel to R-APS VLAN 200, and enable the ERPS function for the Ethernet ring.
  - Configure subring R-APS VLAN 300, add GigabitEthernet 0/4 and virtual channel to R-APS VLAN 300, and enable the ERPS function for the Ethernet ring.
  - Configure subring R-APS VLAN 400, add GigabitEthernet 0/5 and virtual channel to R-APS VLAN 400, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.
- Node 5 is the non-intersecting single-ring node of the subring ERPS 2, as well as the RPL owner node of ERPS 2. Notes for configuring this node are as follows:
  - Configure the subring R-APS VLAN 200, add GigabitEthernet 0/1 and GigabitEthernet 0/2 to R-APS VLAN 200, configure GigabitEthernet 0/1 as the RPL port, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.
- Node 6 is the non-intersecting node of the subring ERPS 3, as well as the RPL owner node of ERPS 3.

Notes for configuring this node are as follows:

- Configure the subring R-APS VLAN 300, add GigabitEthernet 0/1 and GigabitEthernet 0/2 to R-APS VLAN 300, configure GigabitEthernet 0/1 as the RPL port, and enable the ERPS function for the Ethernet ring.
- Enable the global ERPS function.

- Node 7 is the non-intersecting single-ring node of the subring ERPS 4, as well as the RPL owner node of ERPS 4. Notes for configuring this node are as follows:
  - Configure the subring R-APS VLAN 400, add GigabitEthernet 0/1 and GigabitEthernet 0/2 to R-APS VLAN 400, configure GigabitEthernet 0/1 as the RPL port, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.

4. Procedure

(1) Configure node 1.

Configure the major ring ERPS 1 of the intersecting rings. Create a control VLAN (R-APS VLAN 100), add physical ports to the Ethernet ring, configure the east port as the RPL owner port, associate the major ring R-APS VLAN 100 with subrings R-APS VLANs 200, 300, and 400, and enable the ERPS function.

```
Node1> enable
Node1# configure terminal
Node1(config)# interface rang gigabitethernet 0/1-2
Node1(config-if-range)# switchport mode trunk
Node1(config-if-range)# exit
Node1(config)# erps raps-vlan 100
Node1(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node1(config-erps 100)# rpl-port east rpl-owner
Node1(config-erps 100)# exit
Node1(config-erps 100)# associate sub-ring raps-vlan 200,300,400
Node1(config-erps 100)# state enable
Node1(config-erps 100)# exit
```

Configure the subring ERPS 4 of the intersecting rings. Create a control VLAN (R-APS VLAN400), add physical ports to the Ethernet ring, and enable the ERPS function.

```
Node1(config)# interface rang gigabitethernet 0/5
Node1(config-if-range)# switchport mode trunk
Node1(config-if-range)# exit
Node1(config)# erps raps-vlan 400
Node1(config-erps 400)# ring-port west gigabitethernet 0/5 east virtual-channel
Node1(config-erps 400)# state enable
Node1(config-erps 400)# exit
```

Enable the global ERPS function.

```
Node1(config)# erps enable
```

(2) Configure node 2.

Configure R-APS VLAN 100, add physical ports to the Ethernet ring, associate the major ring R-APS VLAN 100 with subrings R-APS VLANs 200, 300, and 400, and enable the ERPS function.

```
Node2> enable
Node2# configure terminal
Node2(config)# interface rang gigabitethernet 0/1-2
Node2(config-if-range)# switchport mode trunk
Node2(config-if-range)# exit
Node2(config)# erps raps-vlan 100
Node2(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node2(config-erps 100)# associate sub-ring raps-vlan 200,300,400
Node2(config-erps 100)# state enable
Node2(config-erps 100)# exit
```

Enable the global ERPS function.

```
Node2(config)# erps enable
```

(3) Configure node 3.

Configure the link mode for Ethernet ring ports, configure the major ring R-APS VLAN 100, add physical ports to the Ethernet ring, associate the major ring R-APS VLAN 100 with subrings R-APS VLANs 200, 300, and 400, and enable the ERPS function.

```
Node3> enable
Node3# configure terminal
Node3(config)# interface range gigabitethernet 0/1-2
Node3(config-if-range)# switchport mode trunk
Node3(config-if-range)# exit
Node3(config)# erps raps-vlan 100
Node3(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node3(config-erps 100)# associate sub-ring raps-vlan 200,300,400
Node3(config-erps 100)# state enable
Node3(config-erps 100)# exit
```

Configure the link mode for ports in ERPS 2, configure an R-APS VLAN for ERPS 2, add physical ports to the subring, and enable the ERPS function.

```
Node3(config)# interface gigabitethernet 0/3
Node3(config-if-GigabitEthernet 0/3)# switchport mode trunk
Node3(config-if-GigabitEthernet 0/3)# exit
Node3(config)# erps raps-vlan 200
Node3(config-erps 200)# ring-port west virtual-channel east gigabitethernet 0/3
Node3(config-erps 200)# state enable
Node3(config-erps 200)# exit
```

Configure the link mode for ports in ERPS 3, configure an R-APS VLAN for ERPS 3, add physical ports to the subring, and enable the ERPS function.

```
Node3(config)# interface gigabitethernet 0/4
Node3(config-if-GigabitEthernet 0/4)# switchport mode trunk
```

```
Node3(config-if-GigabitEthernet 0/4)# exit
Node3(config)# erps raps-vlan 300
Node3(config-erps 300)# ring-port west virtual-channel east gigabitethernet 0/4
Node3(config-erps 300)# state enable
Node3(config-erps 300)# exit
```

Enable the global ERPS function.

```
Node3(config)# erps enable
```

(4) Configure node 4.

Configure the link mode for ports in the major ring, configure R-APS VLAN 100, add physical ports to the Ethernet ring, associate the major ring R-APS VLAN 100 with subrings R-APS VLANs 200, 300, and 400, and enable the ERPS function.

```
Node4> enable
Node4# configure terminal
Node4(config)# interface range gigabitethernet 0/1-2
Node4(config-if-range)# switchport mode trunk
Node4(config-if-range)# exit
Node4(config)# erps raps-vlan 100
Node4(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node4(config-erps 100)# associate sub-ring raps-vlan 200,300,400
Node4(config-erps 100)# state enable
Node4(config-erps 100)# exit
```

Configure the link mode for ports in subring ERPS 2, configure an R-APS VLAN for subring ERPS 2, add physical ports to the subring, and enable the ERPS function.

```
Node4(config)# interface gigabitethernet 0/3
Node4(config-if-GigabitEthernet 0/3)# switchport mode trunk
Node4(config-if-GigabitEthernet 0/3)# exit
Node4(config)# erps raps-vlan 200
Node4(config-erps 200)# ring-port west virtual-channel east gigabitethernet 0/3
Node4(config-erps 200)# state enable
Node4(config-erps 200)# exit
```

Configure the link mode for ports in subring ERPS 3, configure an R-APS VLAN for subring ERPS 3, add physical ports to the subring, and enable the ERPS function.

```
Node4(config)# interface gigabitethernet 0/4
Node4(config-if-GigabitEthernet 0/4)# switchport mode trunk
Node4(config-if-GigabitEthernet 0/4)# exit
Node4(config)# erps raps-vlan 300
Node4(config-erps 300)# ring-port west virtual-channel east gigabitethernet 0/4
Node4(config-erps 300)# state enable
Node4(config-erps 300)# exit
```

Configure the link mode for ports in subring ERPS 4, configure an R-APS VLAN for subring ERPS 4, add physical ports to the subring, and enable the ERPS function.

```
Node4(config)# interface gigabitethernet 0/5
```

```
Node4(config-if-GigabitEthernet 0/5)# switchport mode trunk
Node4(config-if-GigabitEthernet 0/5)# exit
Node4(config)# erps raps-vlan 400
Node4(config-erps 400)# ring-port west virtual-channel east gigabitethernet 0/5
Node4(config-erps 400)# state enable
Node4(config-erps 400)# exit
```

Enable the global ERPS function.

```
Node4(config)# erps enable
```

(5) Configure node 5.

Configure the link mode for Ethernet ring ports, configure an R-APS VLAN, add physical ports to the ring, configure GigabitEthernet 0/1 as the RPL port, and enable the ERPS function.

```
Node5> enable
Node5# configure terminal
Node5(config)# interface range gigabitethernet 0/1-2
Node5(config-if-range)# switchport mode trunk
Node5(config-if-range)# exit
Node5(config)# erps raps-vlan 200
Node5(config-erps 200)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node5(config-erps 200)# rpl-port west rpl-owner
Node5(config-erps 200)# state enable
Node5(config-erps 200)# exit
```

Enable the global ERPS function.

```
Node5(config)# erps enable
```

(6) Configure node 6.

Configure the link mode for Ethernet ring ports, configure an R-APS VLAN, add physical ports to the ring, configure GigabitEthernet 0/1 as the RPL port, and enable the ERPS function.

```
Node6> enable
Node6# configure terminal
Node6(config)# interface range gigabitethernet 0/1-2
Node6(config-if-range)# switchport mode trunk
Node6(config-if-range)# exit
Node6(config)# erps raps-vlan 300
Node6(config-erps 300)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node6(config-erps 300)# rpl-port west rpl-owner
Node6(config-erps 300)# state enable
Node6(config-erps 300)# exit
```

Enable the global ERPS function.

```
Node6(config)# erps enable
```

(7) Configure node 7.

Configure the link mode for Ethernet ring ports, configure an R-APS VLAN, add physical ports to the ring, configure GigabitEthernet 0/1 as the RPL port, and enable the ERPS function.

```
Node7> enable
Node7# configure terminal
Node7(config)# interface range gigabitethernet 0/1-2
Node7(config-if-range)# switchport mode trunk
Node7(config-if-range)# exit
Node7(config)# erps raps-vlan 400
Node7(config-erps 400)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node7(config-erps 400)# rpl-port west rpl-owner
Node7(config-erps 400)# state enable
Node7(config-erps 400)# exit
```

Enable the global ERPS function.

```
Node7(config)# erps enable
```

5. Verification

Run the **show erps** command on each node to verify the configuration. The following uses node 3 as an example.

```
Node3# show erps
ERPS Information
Global Status                 : Enabled
Link monitored by             : Not Oam
--------------------------------------------
R-APS VLAN                    : 200
Ring Status                   : Enabled
West Port                     : Virtual Channel
East Port                     : Gi 0/3 (Forwarding)
RPL Port                      : None
Protected VLANs               : ALL
RPL Owner                     : Disabled
Holdoff Time                  : 0 milliseconds
Guard Time                    : 500 milliseconds
WTR Time                      : 2 minutes
Current Ring State            : Idle
Associate R-APS VLAN          :
--------------------------------------------
R-APS VLAN                    : 300
Ring Status                   : Enabled
West Port                     : Virtual Channel
East Port                     : Gi 0/4 (Forwarding)
RPL Port                      : None
Protected VLANs               : ALL
RPL Owner                     : Disabled
Holdoff Time                  : 0 milliseconds
Guard Time                    : 500 milliseconds
WTR Time                      : 2 minutes
```

```
Current Ring State            : Idle
Associate R-APS VLAN          :
---------------------------------------------
R-APS VLAN                    : 100
Ring Status                   : Enabled
West Port                     : Gi 0/1 (Forwarding)
East Port                     : Gi 0/2 (Blocking)
RPL Port                      : East Port
Protected VLANs               : ALL
RPL Owner                     : Disabled
Holdoff Time                  : 0 milliseconds
Guard Time                    : 500 milliseconds
WTR Time                      : 2 minutes
Current Ring State            : Idle
Associate R-APS VLAN          : 200,300,400
```

6. Common Errors

- An R-APS ring has been enabled but ERPS is not enabled globally, so ERPS does not take effect yet.
- Multiple RPL owner nodes are configured in one ERPS ring.
- Different R-APS VLANs are configured for the nodes in one ERPS ring.
- The nodes in the major ring are not associated with its subring.

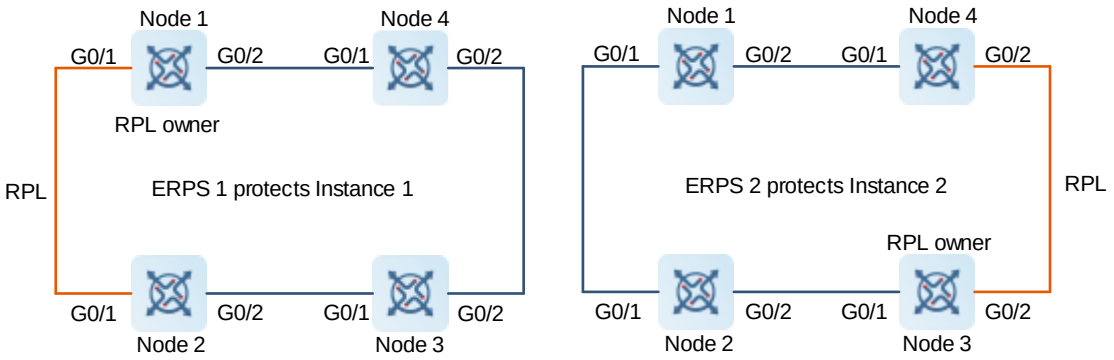
1.13.4 Configuring Load Balancing

1. Requirements

As shown in Figure 1-8, two Ethernet rings are configured in the same physical network: ERPS 1 (nodes 1-2-3-4) protects VLANs 1-2000, and ERPS 2 (nodes 3-4-1-2) protects VLANs 2001-4094.

2. Topology

Figure 1-8 Application Scenario of Load Balancing



3. Notes

- Before adding a physical port to an Ethernet ring, configure the link of the member port to work in trunk mode.
- Before configuring the protected VLANs, create Instances 1 and 2 on nodes 1-4, and map instance 1 to

VLANs 1-2000 and instance 2 to VLANs 2001-4094.

- ERPS 1 and ERPS 2 enabled with load balancing pass through node 1 and node 1 is the RPL owner node of ERPS 1. Notes when configuring this node are as follows:
  - Configure R-APS VLAN 100, add physical ports GigabitEthernet 0/1 and 0/2 to the Ethernet ring, configure GigabitEthernet 0/1 as the RPL port, configure the Ethernet ring to protect VLANs corresponding to instance 1, and enable the ERPS function for the Ethernet ring.
  - Configure R-APS VLAN 200, add physical ports GigabitEthernet 0/1 and GigabitEthernet 0/2 to the Ethernet ring, configure VLANs corresponding to instance 2 protected by the Ethernet ring, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.
- ERPS 1 and ERPS2 with load balancing enabled pass through node 2 and node 4, and node 2 and node 4 are non-RPL owner nodes. Notes for configuring these nodes are as follows:
  - Configure R-APS VLAN 100, add physical ports GigabitEthernet 0/1 and GigabitEthernet 0/2 to the Ethernet ring, configure VLANs corresponding to instance 1 protected by the Ethernet ring, and enable the ERPS function for the Ethernet ring.
  - Configure R-APS VLAN 200, add physical ports GigabitEthernet 0/1 and GigabitEthernet 0/2 to the Ethernet ring, configure VLANs corresponding to instance 2 protected by the Ethernet ring, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.
- ERPS 1 and ERPS 2 enabled with load balancing pass through node 3 and node 3 is the RPL owner node of ERPS 2. Notes for configuring this node are as follows:
  - Configure R-APS VLAN 100, add physical ports GigabitEthernet 0/1 and GigabitEthernet 0/2 to the Ethernet ring, configure VLANs corresponding to instance 1 protected by the Ethernet ring, and enable the ERPS function for the Ethernet ring.
  - Configure R-APS VLAN 200, add physical ports GigabitEthernet 0/1 and GigabitEthernet 0/2 to the Ethernet ring, configure GigabitEthernet 0/2 as the RPL port, configure VLANs corresponding to instance 2 protected by the Ethernet ring, and enable the ERPS function for the Ethernet ring.
  - Enable the global ERPS function.

4. Procedure

(1) Create instance 1 and instance 2, and add protected VLAN groups to the instances. Nodes 1-4 are configured in the same way.

Configure node 1.

```
Node1> enable
Node1# configure terminal
Node1(config)# spanning-tree mst configuration
Node1(config-mst)# instance 1 vlan 1-2000
Node1(config-mst)# instance 2 vlan 2001-4094
Node1(config-mst)# exit
```

Configure node 2.

```
Node2> enable
```

```
Node2# configure terminal
Node2(config)# spanning-tree mst configuration
Node2(config-mst)# instance 1 vlan 1-2000
Node2(config-mst)# instance 2 vlan 2001-4094
Node2(config-mst)# exit
```

Configure node 3.

```
Node3> enable
Node3# configure terminal
Node3(config)# spanning-tree mst configuration
Node3(config-mst)# instance 1 vlan 1-2000
Node3(config-mst)# instance 2 vlan 2001-4094
Node3(config-mst)# exit
```

Configure node 4.

```
Node4> enable
Node4# configure terminal
Node4(config)# spanning-tree mst configuration
Node4(config-mst)# instance 1 vlan 1-2000
Node4(config-mst)# instance 2 vlan 2001-4094
Node4(config-mst)# exit
```

(2) Configure a single-ring node, namely, node 1.

Configure the links of the Ethernet ring ports (GigabitEthernet 0/1 and GigabitEthernet 0/2) to work in trunk mode.

```
Node1(config)# interface range gigabitethernet 0/1-2
Node1(config-if-rang)# switchport mode trunk
Node1(config-if-rang)# exit
```

Configure VLANs in instance 1 protected by ERPS 1.

```
Node1(config)# erps raps-vlan 100
Node1(config-erps 100)# protected-instance 1
Node1(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node1(config-erps 100)# rpl-port west rpl-owner
Node1(config-erps 100)# state enable
Node1(config-erps 100)# exit
```

Configure VLANs in instance 2 protected by ERPS 2.

```
Node1(config)# erps raps-vlan 200
Node1(config-erps 200)# protected-instance 2
Node1(config-erps 200)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node1(config-erps 200)# state enable
Node1(config-erps 200)# exit
```

Enable the global ERPS function.

```
Node1(config)# erps enable
```

(3) Configure a single-ring node, namely, node 2. The configuration commands are the same as those on node 1, except that no RPL needs to be configured.

Configure the links of the Ethernet ring ports (GigabitEthernet 0/1 and GigabitEthernet 0/2) to work in trunk mode.

```
Node2(config)# interface range gigabitethernet 0/1-2
Node2(config-if-rang)# switchport mode trunk
Node2(config-if-rang)# exit
```

Configure VLANs in instance 1 protected by ERPS 1, add the ports to the ring, specify the RPL owner port, and enable the ERPS function.

```
Node2(config)# erps raps-vlan 100
Node2(config-erps 100)# protected-instance 1
Node2(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node2(config-erps 100)# state enable
Node2(config-erps 100)# exit
```

Configure VLANs in instance 2 protected by ERPS 2, add the ports to the Ethernet ring, and enable the ERPS function.

```
Node2(config)# erps raps-vlan 200
Node2(config-erps 200)# protected-instance 2
Node2(config-erps 200)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node2(config-erps 200)# state enable
Node2(config-erps 200)# exit
```

Enable the global ERPS function.

```
Node2(config)# erps enable
```

(4) Configure a single-ring node, namely, node 3. The commands are the same as those on node 1, except that the RPL owner port is configured on ERPS 2.

Configure the links of the Ethernet ring ports (GigabitEthernet 0/1 and GigabitEthernet 0/2) to work in trunk mode.

```
Node3(config)# interface range gigabitethernet 0/1-2
Node3(config-if-rang)# switchport mode trunk
Node3(config-if-rang)# exit
```

Configure VLANs in instance 1 protected by ERPS 1, add the ports to the ring, specify the RPL owner port, and enable the ERPS function.

```
Node3(config)# erps raps-vlan 100
Node3(config-erps 100)# protected-instance 1
Node3(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node3(config-erps 100)# state enable
Node3(config-erps 100)# exit
```

Configure VLANs in instance 2 protected by ERPS 2, add the ports to the Ethernet ring, and enable the ERPS function.

```
Node3(config)# erps raps-vlan 200
Node3(config-erps 200)# protected-instance 2
Node3(config-erps 200)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node3(config-erps 200)# rpl-port east rpl-owner
Node3(config-erps 200)# state enable
Node3(config-erps 200)# exit
```

Enable the global ERPS function.

```
Node3(config)# erps enable
```

(5) Configure a single-ring node, namely, node 4. The configuration is the same as that on node 2.

Configure the links of the Ethernet ring ports (GigabitEthernet 0/1 and GigabitEthernet 0/2) to work in trunk mode.

```
Node4(config)# interface range gigabitethernet 0/1-2
Node4(config-if-rang)# switchport mode trunk
Node4(config-if-rang)# exit
```

Configure VLANs in instance 1 protected by ERPS 1, add the ports to the ring, specify the RPL owner port, and enable the ERPS function.

```
Node4(config)# erps raps-vlan 100
Node4(config-erps 100)# protected-instance 1
Node4(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node4(config-erps 100)# state enable
Node4(config-erps 100)# exit
```

Configure VLANs in instance 2 protected by ERPS 2, add the ports to the Ethernet ring, and enable the ERPS function.

```
Node4(config)# erps raps-vlan 200
Node4(config-erps 200)# protected-instance 2
Node4(config-erps 200)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/2
Node4(config-erps 200)# state enable
Node4(config-erps 200)# exit
```

Enable the global ERPS function.

```
Node4(config)# erps enable
```

5. Verification

Run the **show erps** command on each node to verify the configuration. The following uses the configuration on node 1 as an example.

```
Node1# show erps
ERPS Information
Global Status                 : Enabled
Link monitored by             : Not Oam
---------------------------------------------
R-APS VLAN                    : 100
```

```
Ring Status                    : Enabled
West Port                      : Gi 0/1 (Blocking)
East Port                      : Gi 0/2 (Forwarding)
RPL Port                       : West Port
Protected VLANs                : 1-2000
RPL Owner                      : Enabled
Holdoff Time                   : 0 milliseconds
Guard Time                     : 500 milliseconds
WTR Time                       : 2 minutes
Current Ring State             : Idle
Associate R-APS VLAN           :
---------------------------------------------
R-APS VLAN                     : 200
Ring Status                    : Enabled
West Port                      : Gi 0/1 (Forwarding)
East Port                      : Gi 0/2 (Blocking)
RPL Port                       : West Port
Protected VLANs                : 2001-4094
RPL Owner                      : Enabled
Holdoff Time                   : 0 milliseconds
Guard Time                     : 500 milliseconds
WTR Time                       : 2 minutes
Current Ring State             : Idle
Associate R-APS VLAN           :
```

6. Common Errors

- An R-APS ring has been enabled but ERPS is not enabled globally, so ERPS does not take effect yet.
- Multiple RPL owner nodes are configured in one ERPS ring.
- Different R-APS VLANs are configured for the nodes in one ERPS ring.

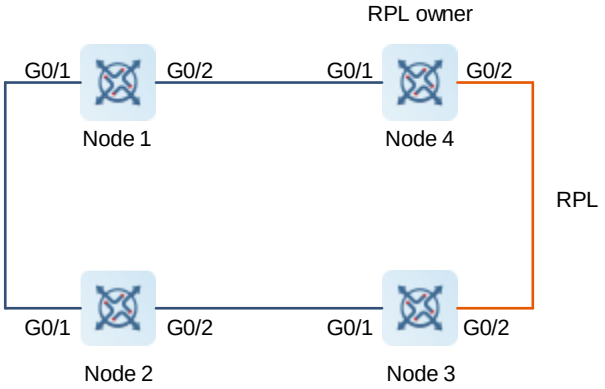
1.13.5 Modifying ERPS Configuration

1. Requirements

ERPS has been configured in a ring. An ERPS port needs to be changed because of a physical topology change.

2. Topology

Figure 1-9 Application Scenario of ERPS Configuration Modification



3. Notes

- Shut down a link in the ring and configure the link mode for the new Ethernet ring port.
- Disable ERPS for the ring in R-APS VLAN mode.
- Reconfigure the ports that will participate in ERPS calculation.
- Enable the ERPS function for this ring.
- Modify the ERPS timers.

4. Procedure

(1) Configure node 1.

In interface configuration mode, shut down a link in the ring to prevent loops.

```
Node1> enable
Node1# configure terminal
Node1(config)# interface gigabitethernet 0/1
Node1(config-if-GigabitEthernet 0/1)# shutdown
Node1(config-if-GigabitEthernet 0/1)# exit
```

Configure the link mode for the new Ethernet ring port.

```
Node1(config)# interface gigabitethernet 0/3
Node1(config-if-GigabitEthernet 0/3)# switchport mode trunk
Node1(config-if-GigabitEthernet 0/3)# exit
```

Enter the R-APS VLAN configuration mode, disable the ERPS function and delete previous ring configurations.

```
Node1(config)# erps raps-vlan 100
Node1(config-erps 100)# no state enable
Node1(config-erps 100)# no ring-port
```

Modify the configuration of Ethernet ring ports, change GigabitEthernet 0/2 to GigabitEthernet 0/3, and enable the ERPS function.

```
Node1(config-erps 100)# ring-port west gigabitethernet 0/1 east gigabitethernet
0/3
```

```
Node1(config-erps 100)# state enable
Node1(config-erps 100)# exit
```

Enable the port that is previously disabled.

```
Node1(config)# interface gigabitethernet 0/1
Node1(config-if-GigabitEthernet 0/1)# no shutdown
```

(2) Configure node 4, enter the ERPS configuration mode, and modify timers.

```
Node4> enable
Node4# configure terminal
Node4(config)# erps raps-vlan 100
Node4(config-erps 100)# timer wtr-time 1
```

5. Verification

Wait for 1 minute. After the ERPS ring is restored to the idle state, run the **show erps** command on node 1 to verify the configuration.

```
Node1# show erps
ERPS Information
Global Status                 : Enabled
Link monitored by             : Not Oam
--------------------------------------------
R-APS VLAN                    : 100
Ring Status                   : Enabled
West Port                     : Gi 0/1 (Forwardin)
East Port                     : Gi 0/3 (Forwardin)
RPL Port                      : None
Protected VLANs               : ALL
RPL Owner                     : Enabled
Holdoff Time                  : 0 milliseconds
Guard Time                    : 500 milliseconds
WTR Time                  : 2 minutes
Current Ring State            : Idle
Associate R-APS VLAN          :
```

Wait for 1 minute. After the ERPS ring is restored to the idle state, run the **show erps** command on node 4 to verify the configuration.

```
Node4# show erps
ERPS Information
Global Status                 : Enabled
Link monitored by             : Not Oam
--------------------------------------------
R-APS VLAN                    : 100
Ring Status                   : Enabled
West Port                     : Gi 0/1 (Forwardin)
East Port                     : Gi 0/2 (Blocking)
RPL Port                      : East Port
Protected VLANs               : ALL
```

```
RPL Owner                    : Enabled
Holdoff Time                 : 0 milliseconds
Guard Time                   : 500 milliseconds
WTR Time                  : 1 minutes
Current Ring State           : Idle
Associate R-APS VLAN         :
```

6. Common Errors

- The R-APS ring is not enabled after the configuration is modified.
- The ports that are previously disabled are not enabled after the configuration is modified.

Contents

1 Configuring LLDP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 LLDP Packet 1
1.1.3 TLV Type 2
1.1.4 LLDP Work Mode 5
1.1.5 LLDP Packet Transmission Mechanism 5
1.1.6 LLDP Packet Receiving Mechanism 6
1.1.7 Protocols and Standards 6
1.2 Configuration Task Summary 6
1.3 Enabling the LLDP Function 6
1.3.1 Overview 6
1.3.2 Restrictions and Guidelines 7
1.3.3 Procedure 7
1.4 Configuring the LLDP Work Mode 7
1.4.1 Overview 7
1.4.2 Restrictions and Guidelines 7
1.4.3 Procedure 8
1.5 Configuring an Interface Initialization Delay 8
1.5.1 Overview 8
1.5.2 Procedure 8
1.6 Configuring the TLVs to Be Advertised 8
1.6.1 Overview 8

1.6.2 Restrictions and Guidelines 8

1.6.3 Procedure 10

1.7 Configuring the Management Address to Be Advertised in LLDP Packets 10

1.7.1 Overview 10

1.7.2 Restrictions and Guidelines 10

1.7.3 Procedure 10

1.8 Configuring the LLDP Packet Encapsulation Format 11

1.8.1 Overview 11

1.8.2 Procedure 11

1.9 Configuring the Number of LLDP Packets That Can Be Transmitted Rapidly 11

1.9.1 Overview 11

1.9.2 Procedure 11

1.10 Configuring the TTL Multiplier and LLDP Packet Transmission Interval 12

1.10.1 Overview 12

1.10.2 Restrictions and Guidelines 12

1.10.3 Procedure 12

1.11 Configuring an LLDP Packet Transmission Delay 13

1.11.1 Overview 13

1.11.2 Restrictions and Guidelines 13

1.11.3 Procedure 13

1.12 Configuring the Function of Ignoring PVID Detection 13

1.12.1 Overview 13

1.12.2 Procedure 13

1.13 Configuring the Function of Being Compatible with the Neighbor Discovery of Vendors' Devices 14

1.13.1 Overview 14

1.13.2 Procedure 14

1.14 Configuring the LLDP Trap Function 14

1.14.1 Overview 14

1.14.2 Procedure 14

1.15 Configuring the LLDP Error Detection Function 15

1.15.1 Overview 15

1.15.2 Restrictions and Guidelines 15

1.15.3 Procedure 15

1.16 Configuring the Civic Address 15

1.16.1 Overview 15

1.16.2 Restrictions and Guidelines 15

1.16.3 Procedure 16

1.17 Configuring the Emergency Telephone Number 16

1.17.1 Overview 16

1.17.2 Procedure 16

1.18 Configuring an LLDP Network Policy 17

1.18.1 Overview 17

1.18.2 Restrictions and Guidelines 17

1.18.3 Procedure 17

1.19 Monitoring 18

1.20 Configuration Examples 19

1.20.1 Checking the Neighbors Connected to the Device by Using the LLDP Function 19

1.20.2 Configuring the LLDP Error Detection Function 21

1 Configuring LLDP

1.1 Introduction

1.1.1 Overview

The Link Layer Discovery Protocol (LLDP) is a L2 discovery protocol defined in the IEEE 802.1AB standard. It is used to discover a topology and identify topological changes. LLDP encapsulates local information of a device into LLDP data units (LLDPDUs) in the type length value (TLV) format and then sends the LLDPDUs to neighbors. It also stores LLDPDUs from neighbors in the management information base (MIB) to be accessed by the network management system (NMS).

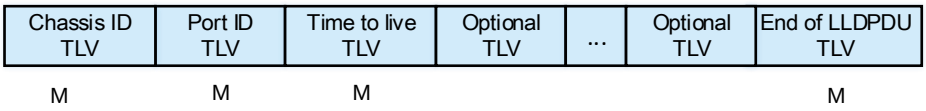
With LLDP, the NMS can learn about topology connections, for example, interfaces of a device connected to other devices, as well as the rates and duplex modes of interfaces at both ends of a link. Administrators can quickly locate and eliminate a fault based on the information. An LLDP-compliant device is capable of discovering neighbors when its peer is either an LLDP-compliant device or a device supporting the Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED).

1.1.2 LLDP Packet

An LLDP-compliant device advertises its status information by using different TLV combinations, and obtains status information of neighbors. A series of TLV combinations are encapsulated into LLDPDUs, which then are encapsulated in LLDP packets for transmission.

Figure 1-1 shows the format of an LLDPDU, wherein M indicates a mandatory TLV. As specified in LLDP, each LLDPDU can contain 28 types of TLVs, and always starts with the chassis ID TLV, port ID TLV, and Time To Live (TTL) TLV, and ends with the end of LLDPDU TLV. Other types of TLVs are optional.

Figure 1-1 LLDPDU Format



LLDP packets can be encapsulated in two formats: Ethernet II and Sub Network Access Protocols (SNAP).

Figure 1-2 shows an LLDP packet encapsulated in Ethernet II format. Table 1-1 describes the related fields.

Figure 1-2 LLDP Packet Encapsulated in Ethernet II Format

Table 1-1 Description of Fields in an LLDP Packet Encapsulated in Ethernet II Format

Field	Description
Destination Address	Destination address, which is a fixed multicast address: 0180.c200.000e.
Source Address	Source MAC address, which is the interface MAC address of the device.

Field	Description
Ether type	Ethernet type, which is 0x88CC.
LLDPDU	LLDP data unit.
FCS	Frame check sequence.

Figure 1-3 shows an LLDP packet encapsulated in SNAP format. Table 1-2 describes the related fields.

Figure 1-3 LLDP Packet Encapsulated in SNAP Format

Destination address	Source address	SNAP-encoded Ethertype	LLDPDU	FCS

Table 1-2 Description of Fields in an LLDP Packet Encapsulated in SNAP Format

Field	Description
Destination Address	Destination address, which is a fixed multicast address: 0180.c200.000e.
Source Address	Source MAC address, which is the interface MAC address of the device.
SNAP-encoded Ether type	SNAP-encapsulated Ethernet type, which is AA-AA-03-00-00-00-88-CC.
LLDPDU	LLDP data unit.
FCS	Frame check sequence.

1.1.3 TLV Type

TLVs encapsulated in LLDPDUs are classified into basic management TLVs and organizationally specific TLVs.

1. Basic Management TLVs

Basic management TLVs are a collection of basic TLVs used for network management. This collection consists of two types of TLVs: mandatory TLVs and optional TLVs. A mandatory TLV must be contained in an LLDPDU for advertisement and an optional TLV is contained selectively. Table 1-3 describes the types of basic management TLVs.

Table 1-3 Basic Management TLVs

TLV Type	Description	Mandatory/Optional
End Of LLDPDU TLV	End flag of an LLDPDU, occupying two bytes.	Mandatory
Chassis ID TLV	Device ID, represented using a MAC address.	Mandatory
Port ID TLV	Interface sending an LLDPDU.	Mandatory
Time To Live TLV	TTL of local information on a neighbor. When a device receives a TLV with TTL of 0, it deletes the neighbor information.	Mandatory

TLV Type	Description	Mandatory/Optional
Port Description TLV	Descriptor of the interface sending an LLDPDU.	Optional
System Name TLV	Device name.	Optional
System Description TLV	Device description, including the hardware version, software version, and operating system.	Optional
System Capabilities TLV	Main functions supported by the device, such as the bridge, routing, and relay functions.	Optional
Management Address TLV	Management address, which contains the interface ID and object identifier (OID).	Optional

Note

This LLDP-compliant device supports advertisement of basic management TLVs.

2. Organizationally Specific TLVs

Organizationally specific TLVs are defined by standard organizations and other institutions, for example, the IEEE 802.1 working group, the IEEE 802.3 working group, Internet Engineering Task Force (IETF), and equipment suppliers define their own TLV collections. Different organizations define specific TLVs to advertise specific information about devices. The organizationally unique identifier (OUI) field in a TLV is used to distinguish different organizations.

Organizationally specific TLVs are optional and are advertised in an LLDPDU selectively. Currently, there are three types of common organizationally specific TLVs: IEEE 802.1 organizationally specific TLVs, IEEE 802.3 organizationally specific TLVs, and LLDP-MED TLVs.

- Table 1-4 describes IEEE 802.1 organizationally specific TLVs.

Table 1-4 IEEE 802.1 Organizationally Specific TLVs

TLV Type	Description
Port VLAN ID TLV	Virtual local area network (VLAN) identifier of an interface.
Port And Protocol VLAN ID TLV	Protocol VLAN identifier of an interface.
VLAN Name TLV	VLAN name of an interface.
Protocol Identity TLV	Protocol type supported by an interface.

Note

This LLDP-compliant device does not send the protocol identity TLV but receives this TLV.

- Table 1-5 describes IEEE 802.3 organizationally specific TLVs.

Table 1-5 IEEE 802.3 Organizationally Specific TLVs

TLV Type	Description
MAC/PHY Configuration//Status TLV	Rate and duplex mode of an interface, and whether auto-negotiation is supported and enabled.
Power Via MDI TLV	Power supply capacity of an interface.
Link Aggregation TLV	Link aggregation capacity of an interface and the current aggregation state.
Maximum Frame Size TLV	Maximum size of the frame that can be transmitted by an interface.

Note

This LLDP-compliant device supports advertisement of IEEE 802.3 organizationally specific TLVs.

- LLDP-MED TLV

LLDP-MED is an extension to LLDP based on IEEE 802.1AB LLDP. It enables users to conveniently deploy the Voice over IP (VoIP) network and detect faults. It provides applications including the network configuration policies, device discovery, Power over Ethernet (PoE) management, and inventory management, which can meet requirements for low cost, effective management, and easy deployment and help simplify deployment of audio devices. Table 1-6 describes LLDP-MED TLVs.

Table 1-6 LLDP-MED TLV

TLV Type	Description
LLDP-MED Capabilities TLV	Whether the device supports LLDP-MED, the type of the LLDP-MED TLV encapsulated into an LLDPDU, and device type (network connectivity device or endpoint device).
Network Policy TLV	Interface VLAN configuration, supported application type (such as voice or video services), and L2 priority information.
Location Identification TLV	Endpoint device ID. An endpoint device can be accurately located in network topology collection and other applications.
Extended Power-via-MDI TLV	More advanced power supply management.
Inventory – Hardware Revision TLV	Hardware version of a MED device.
Inventory – Firmware Revision TLV	Firmware version of a MED device.
Inventory – Software Revision TLV	Software version of a MED device.
Inventory – Serial Number TLV	Serial number of a MED device.
Inventory – Manufacturer Name TLV	Name of the manufacturer of a MED device.
Inventory – Model Name TLV	Module name of a MED device.

TLV Type	Description
Inventory – Asset ID TLV	Asset identifier of a MED device, used for inventory management and asset tracking.

Note

This LLDP-compliant device supports advertisement of LLDP-MED TLVs.

1.1.4 LLDP Work Mode

LLDP supports three work modes.

- TxRx: Transmits and receives LLDPDUs.
- Rx Only: Only receives LLDPDUs.
- Tx Only: Only transmits LLDPDUs.

Caution

When the LLDP work mode of an interface is changed, the interface initializes the protocol state machine. You can set an interface initialization delay to prevent repeated initialization of an interface due to frequent changes of the LLDP work mode.

1.1.5 LLDP Packet Transmission Mechanism

LLDP-compliant devices can send LLDP packets to peers. LLDP packets are used to inform peers of their neighbors. When the LLDP transmission mode is canceled or the interface is disabled, LLDP packets can inform peers that their neighbors are no longer valid.

LLDP periodically transmits LLDP packets when working in TxRx or Tx Only mode. When information about the local device changes, LLDP immediately transmits LLDP packets. You can configure an LLDP packet transmission delay to avoid frequent transmission of LLDP packets caused by frequent changes of local information. This delay can be manually configured.

LLDP provides two types of packets:

- Standard LLDP packet: It contains management and configuration information of the local device.
- Shutdown packet: When the LLDP work mode is disabled or the interface is shut down, LLDP shutdown packets will be transmitted. A shutdown packet consists of the chassis ID TLV, port ID TLV, TTL TLV, and end of LLDP TLV. TTL in the TTL TLV is 0. When a device receives an LLDP shutdown packet, it considers the neighbor information invalid and immediately deletes it.

When the LLDP work mode is changed from disabled or Rx to TxRx or Tx, or LLDP discovers a new neighbor (that is, a device receives a new LLDP packet and the neighbor information is not stored locally), the fast transmission mechanism is started so that the neighbor quickly learns the device information. The fast transmission mechanism enables a device to transmit a certain number of LLDP packets at an interval of 1 second.

1.1.6 LLDP Packet Receiving Mechanism

LLDP-compliant devices can receive LLDP packets from the peers. A device can discover its neighbors and determine when to age the neighbor information according to received LLDP packets.

A device can receive LLDP packets when working in TxRx or Rx Only mode. After receiving an LLDP packet, a device conducts a validity check. After the packet passes the check, the device checks whether the packet provides information about a new neighbor or information update of an existing neighbor and stores the neighbor information locally. The device sets the TTL of neighbor information according to the value of TTL TLV in the packet. If the value of TTL TLV is 0, the neighbor information needs to be aged immediately.

1.1.7 Protocols and Standards

- IEEE 802.1AB 2005:IEEE Standard for Local and metropolitan area networks - Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057: Link Layer Discovery Protocol for Media Endpoint Devices

1.2 Configuration Task Summary

The following tasks are optional:

(1) Enabling the LLDP Function

(2) Configuring the LLDP Work Mode

(3) Configuring an Interface Initialization Delay

(4) Configure parameters related to LLDP packets.

- Configuring the TLVs to Be Advertised
- Configuring the Management Address to Be Advertised in LLDP Packets
- Configuring the LLDP Packet Encapsulation Format
- Configuring the Number of LLDP Packets That Can Be Transmitted Rapidly
- Configuring the TTL Multiplier and LLDP Packet Transmission Interval
- Configuring an LLDP Packet Transmission Delay

(5) Configuring the Function of Ignoring PVID Detection

(6) Configuring the Function of Being Compatible with the Neighbor Discovery of Vendors' Devices

(7) Configuring the LLDP Trap Function

(8) Configuring the LLDP Error Detection Function

(9) Configuring the Civic Address

(10) Configuring the Emergency Telephone Number

(11) Configuring an LLDP Network Policy

1.3 Enabling the LLDP Function

1.3.1 Overview

This section describes how to enable or disable the LLDP function globally and on an interface. The LLDP function is enabled globally and on an interface by default. The function configuration is optional.

1.3.2 Restrictions and Guidelines

- To make the LLDP function take effect on an interface, you need to enable the LLDP function globally and on the interface.
- Configuring the LLDP function in global configuration mode will enable the LLDP function globally. Configuring the LLDP function in interface configuration mode will enable the LLDP function on the interface.
- The **lldp enable** command is used to enable the LLDP function. The LLDP function is enabled by default. Therefore, no configuration is required to enable the function. The **no lldp enable** command is used to disable the LLDP function.
- When a neighbor does not support LLDP but it is connected to an LLDP-supported device in downlink direction, an interface may learn information about the device that is not directly connected to the interface because the neighbor may forward LLDP packets.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the global LLDP function.

[**no**] **lldp enable**

The global LLDP function is enabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure the LLDP function for the interface.

[**no**] **lldp enable**

The LLDP function is enabled on interfaces by default.

1.4 Configuring the LLDP Work Mode

1.4.1 Overview

This section describes how to configure the LLDP packet transmission and receiving mode. The device has default configuration and the configuration command of this function is optional.

1.4.2 Restrictions and Guidelines

- LLDP only runs on physical ports. It runs on member ports for an aggregation port. Stacked ports and VSL ports do not support LLDP.
- The default LLDP work mode is **TxRx**, indicating that an interface can transmit and receive LLDPDUs. You can set the LLDP work mode to **Tx** or **Rx** as required. When the **no lldp mode** command is used to disable the LLDP work mode of an interface, the interface neither transmits nor receives LLDP packets.
- When you set the LLDP work mode of an interface to **Tx**, the interface can only transmit packets but cannot receive packets.

- When you set the LLDP work mode of an interface to **Rx**, the interface can only receive packets but cannot transmit packets.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the LLDP work mode.

lldp mode { **rx** | **tx** | **txrx** }

The default LLDP work mode is **TxRx**, indicating that an interface can transmit and receive LLDPDUs.

1.5 Configuring an Interface Initialization Delay

1.5.1 Overview

You can configure an interface initialization delay in global configuration mode to prevent frequent initialization of the state machine caused by frequent changes of the interface work mode.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an interface initialization delay.

lldp timer reinit-delay *reinit*

The default LLDP interface initialization delay is 2 seconds.

1.6 Configuring the TLVs to Be Advertised

1.6.1 Overview

You can configure the type of TLVs to be advertised to specify the LLDPDUs in LLDP packets.

By default, an interface is allowed to advertise TLVs of all types except the Location Identification TLV.

1.6.2 Restrictions and Guidelines

- You can run the **lldp tlv-enable** *tlv-type subtype* command on an interface to configure the type of TLVs to be advertised as required.

  Run the **no lldp tlv-enable** *tlv-type subtype* command to cancel the advertisement of TLVs of the specified types.

- *tlv-type* indicates the TLV type, and one type must be configured; *subtype* indicates the sub-type and one sub-type must be configured. Sub-type varies with *tlv-type*.
  - The value range of the *subtype* parameter for **basic-tlv** (basic management TLVs) is as follows:

    all: Advertises all optional TLVs of this type.

    port-description: Indicates the Port Description TLV.

    system-capability: Indicates the System Capabilities TLV.

    system-description: Indicates the System Description TLV.

    system-name: Indicates the System Name TLV.
  - The value range of the *subtype* parameter for **dot1-tlv** (IEEE 802.1 organizationally specific TLVs) is as follows:

    all: Advertises all optional TLVs of this type.

    port-vlan-id: Indicates the Port VLAN ID TLV.

    protocol-vlan-id [*vlan-id*]: Indicates the Port And Protocol VLAN ID TLV. Where, *vlan-id* indicates the port protocol VLAN ID. The value range is from 1 to 4094.

    vlan-name [*vlan-id*]: Indicates the VLAN Name TLV. Where, *vlan-id* indicates the VLAN ID. The value range is from 1 to 4094.
  - The value range of the *subtype* parameter for **dot3-tlv** (IEEE 802.3 organizationally specific TLVs) is as follows:

    all: Advertises all optional TLVs of this type.

    link-aggregation: Indicates the Link Aggregation TLV.

    mac-physic: Indicates the MAC/PHY Configuration/Status TLV.

    max-frame-size: Indicates the Maximum Frame Size TLV.

    power: Indicates the Power Via MDI TLV.
  - The value range of the *subtype* parameter for **med-tlv** (LLDP-MED TLV) is as follows:

    all: Advertises all types of LLDP-MED TLVs other than the **Location** Identification TLV.

    capability: Indicates the LLDP-MED Capabilities TLV.

    inventory: Indicates the inventory management TLV, which contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier.

    location { **civic-location | elin** } **identifier** *id*: Indicates the Location Identification TLV. Where, **civic-location** encapsulates the civic address information of the network connection device, **elin** encapsulates the emergency telephone number, and **identifier** *id* indicates the policy ID, with the value range from 1 to 1024.

    network-policy profile [*profile-num*]: Indicates the Network Policy TLV. Where, *profile-num* indicates the network policy ID. The value range is from 1 to 1024.

    power-over-ethernet: Indicates the Extended Power-via-MDI TLV.
- Before configuring the advertisement of the LLDP-MED **capability** TLV, configure the device to allow the advertisement of the LLDP IEEE 802.3 **mac-physic** TLV.

  Before canceling the advertisement of the LLDP IEEE 802.3 **mac-physic** TLV, first cancel the advertisement of the LLDP-MED **capability** TLV.

- If you want to configure LLDP-MED TLVs, configure the LLDP-MED **capability** TLV before configuring other types of LLDP-MED TLVs. If you want to cancel the advertisement of LLDP-MED TLVs, cancel the LLDP-MED **capability** TLV before canceling other types of LLDP-MED TLVs. If a device is connected to an IP phone in the downlink direction and the IP phone supports LLDP-MED, you can configure the Network Policy TLV to deliver policies to the IP phone.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the TLVs to be advertised.

lldp tlv-enable *tlv-type subtype*

By default, if a device supports the Data Center Bridging Capability Exchange protocol (DCBX), interfaces are allowed to transmit all types of TLVs except IEEE 802.3 organizationally specific TLVs and LLDP-MED TLVs. If a device does not support DCBX, interfaces are allowed to transmit all types of TLVs except the Location Identification TLV. The default transmission policy is **none** for the Network Policy TLV in LLDP-MED TLVs.

1.7 Configuring the Management Address to Be Advertised in LLDP Packets

1.7.1 Overview

You can configure the management address to be advertised in LLDP packets in global or interface configuration mode.

After the management address to be advertised is canceled, the management address in LLDP packets is set to the default value.

1.7.2 Restrictions and Guidelines

- LLDP runs on physical ports (member ports for an aggregation port). Stacked ports and VSL ports do not support LLDP.
- The management address to be advertised in LLDP packets can be configured in either global configuration mode or interface configuration mode. The management address configured in global configuration mode takes priority over that configured in interface configuration mode. No LLDP management address can be configured for a specific interface if a global LLDP management address is available.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the management address to be advertised in LLDP packets.

lldp management-address-tlv { *ip-address* | *ipv6-address* }

A management address is advertised through LLDP packets according to the following policy by default: The management address is the IPv4 address of the minimum VLAN supported by an interface. If no IPv4 address is configured for the VLAN, LLDP keeps searching for the next allowed minimum VLAN until a qualified IP address is found. If no IPv4 address is found, LLDP searches for the IPv6 address of the minimum VLAN supported by an interface. If no IPv6 address is found, the local address 127.0.0.1 is used as the management address.

1.8 Configuring the LLDP Packet Encapsulation Format

1.8.1 Overview

The same LLDP packet encapsulation format needs to be configured on the local device and its neighbors in interface configuration mode to ensure their normal communication.

1.8.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Set the LLDP packet encapsulation format to SNAP.

lldp encapsulation snap

The default LLDP packet encapsulation format is Ethernet II.

1.9 Configuring the Number of LLDP Packets That Can Be Transmitted Rapidly

1.9.1 Overview

You can configure the number of LLDP packets that can be transmitted rapidly for the fast transmission mechanism.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the number of LLDP packets that can be transmitted rapidly.

lldp fast-count *fast-count-value*

By default, three LLDP packets can be transmitted rapidly.

1.10 Configuring the TTL Multiplier and LLDP Packet Transmission Interval

1.10.1 Overview

In LLDP packets, TTL TLV indicates the TTL of local information on a neighbor.

The value of TTL TLV is calculated using the following formula: TTL TLV = TTL multiplier × Packet transmission interval + 1. The TTL TLV value can be modified by configuring the TTL multiplier and LLDP packet transmission interval. For example, set the TTL multiplier to 2 and the packet transmission interval to 30 seconds. The TTL of local information on a neighbor is 61 seconds (that is, 2 × 30 + 1).

1.10.2 Restrictions and Guidelines

- You can run the **lldp hold-multiplier** *ttl-value* command to configure the TTL multiplier, so as to control the TTL of local information on a neighbor.
- You can run the **lldp timer tx-interval** *txinterval* command to configure the LLDP packet transmission interval. *txinterval* indicates the time interval, in seconds. The value range is from 1 to 32768, and the default value is **30**. For the standard MIB, the LLDP packet transmission interval is 5–32768 seconds. The range is wider on this device to meet the requirements of more scenarios.
- If the interval is set to a very small value, LLDP packets may be transmitted frequently. If the interval is set to a very large value, the peer may not discover the local device in time.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the TTL multiplier.

lldp hold-multiplier *ttl-value*

The default TTL multiplier of LLDP packets is **4**.

(4) Configure the LLDP packet transmission interval.

lldp timer tx-interval *txinterval*

The default LLDP packet transmission interval is **30** seconds.

1.11 Configuring an LLDP Packet Transmission Delay

1.11.1 Overview

When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. You can configure a transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information.

1.11.2 Restrictions and Guidelines

- The default LLDP packet transmission delay is **2** seconds. The **txdelay** parameter is used to configure an LLDP packet transmission delay. The value range is from 1 to 8192.
- If the delay is set to a very small value, frequent change of the local information will cause frequent transmission of LLDP packets. If the delay is set to a very large value, no LLDP packet may be transmitted even if local information is changed. Set an appropriate delay according to actual conditions.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an LLDP packet transmission delay.

lldp timer tx-delay *txdelay*

The default LLDP packet transmission delay is **2** seconds.

1.12 Configuring the Function of Ignoring PVID Detection

1.12.1 Overview

This section describes how to configure the function of ignoring port VLAN ID (PVID) detection.

1.12.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the function of ignoring PVID detection.

lldp ignore pvid-error-detect

The function of ignoring PVID detection is disabled by default.

1.13 Configuring the Function of Being Compatible with the Neighbor Discovery of Vendors' Devices

1.13.1 Overview

This section describes how to configure the function of being compatible with the neighbor discovery of vendors' devices on the device.

1.13.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of being compatible with the neighbor discovery of vendors' devices.

lldp compliance vendor

The function of being compatible with the neighbor discovery of vendors' devices is disabled by default.

1.14 Configuring the LLDP Trap Function

1.14.1 Overview

The LLDP trap function enables a device to send its local LLDP information (such as neighbor discovery and communication link fault) to the NMS server so that administrators learn about the network performance.

You can configure an LLDP trap transmission interval in global configuration mode to prevent frequent transmission of LLDP trap messages. LLDP changes detected within this interval will be transmitted to the NMS server through traps.

1.14.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure an LLDP trap transmission interval.

lldp timer notification-interval *trap*

The default LLDP trap transmission interval is 5 seconds.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Enable the LLDP trap function.

lldp notification remote-change enable

The LLDP trap function is disabled by default.

1.15 Configuring the LLDP Error Detection Function

1.15.1 Overview

After the LLDP error detection function is enabled, when LLDP detects an error, the error is logged.

Error detection includes detecting VLAN configuration at both ends of a link, interface status, aggregation port configuration, maximum transmission unit (MTU) configuration, and loops.

1.15.2 Restrictions and Guidelines

The LLDP error detection function relies on specific TLVs in LLDP packets exchanged between devices at both ends of a link. Therefore, a device needs to advertise correct TLVs to ensure normal operation the LLDP error detection function.

1.15.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the LLDP error detection function.

lldp error-detect

The LLDP error detection function is enabled by default.

1.16 Configuring the Civic Address

1.16.1 Overview

This section describes how to configure a civic address for a device in LLDP civic address configuration mode.

1.16.2 Restrictions and Guidelines

- Run the **lldp location civic-location identifier** *id* command to enter the LLDP civic address configuration mode.
- In LLDP civic address configuration mode, run the **civic-location** command to configure a civic address for a device. Parameters of this command consist of two parts: address type indicated by *ca-type* and address information indicated by *ca-word*. The **civic-location** keyword is not reflected in the configuration command. The configuration starts directly with the *ca-type* parameter. Run the *ca-type ca-word* command to configure the device address, or run the **no** form of this command to delete the corresponding address information.
- Optional parameters for *ca-type* include the following: **country** (country), **state** (state)**, county** (county), **city** (city), **division** (district), **neighborhood** (community), **street-group** (street), **leading-street-dir (street No.), trailing-street-suffix** (street No.), **street-suffix** (street No.), **number** (street No.), **street-number-suffix**(street No.), **landmark** (landmark),**additional-location-information** (additional address), **name** (name), **postal-code** (postal code), **building** (building), **unit** (unit), **floor** (floor), **room**

(room), **type-of-place** (type of place), **postal-community-name** (post office), **post-office-box** (post-office box), and **additional-code** (additional code).

- The *ca-word* parameter is used to configure address information. When the address type is **country**, address information can use only two characters to represent a country. For example, **country** CH represents China.
- In LLDP civic address configuration mode, run the **device-type** *device-type* command to configure the device type. The default value of *device-type* is 1. The parameter can be set to **0** to indicate a DHCP server, **1** to indicate a switch, and **2** to indicate an LLDP-MED device.Run the **no device-type** to restore the default configuration.

1.16.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the civic address configuration mode of LLDP-MED TLVs.

lldp location civic-location identifier *id*

(4) Configure the address information.

{ **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** } *ca-word*

No address information is configured by default.

(5) Configure the device information.

device-type *device-type*

No device type is configured by default.

1.17 Configuring the Emergency Telephone Number

1.17.1 Overview

You can configure the emergency telephone number information for a device as needed.

1.17.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the emergency telephone number for the device.

lldp location elin identifier *id* **elin-location** *tel-number*

1.18 Configuring an LLDP Network Policy

1.18.1 Overview

If the downlink IP phone supports LLDP, the IP phone will actively transmit LLDP packets when it goes online. If the device is configured with the LLDP network policy TLV, it can capture LLDP packets sent from the IP phone and transmit a voice VLAN policy to the IP phone. If the policy requires the IP phone to send tagged frames and the IP phone supports tagged packets, it will add VLAN tags when transmitting voice packets as per the policy. If the policy requires the IP phone to send untagged frames, the IP phone will transmit untagged packets.

1.18.2 Restrictions and Guidelines

In addition to creating an LLDP network policy on a device, you also need to:

- Enable the voice VLAN function, and add the interface connected to the IP phone to the voice VLAN statically. If the downlink IP phone does not support LLDP-MED, manually add the MAC address of the IP phone to the voice VLAN OUI list. For details, see the *Configuring Voice VLAN*.
- Configure the QoS module to trust the priority modified by the port. For details, see "Configuring QoS" in "ACL and QoS."
- If 802.1x authentication is also enabled on this port, you also need to configure a secure channel to allow packets in the voice VLAN to pass. For details, see "Configuring ACL" in "ACL and QoS".

1.18.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an LLDP network policy and enter the configuration mode.

lldp network-policy profile *profile-num*

No LLDP network policy is configured by default.

(4) Configure a voice VLAN policy. Select at least one of the following to configure:

- Configure the IP phone to transmit tagged frames.

  { **voice** | **voice-signaling** } **vlan** { *voice-vlan-id* | **dot1p** } [**cos** *cos* | **dscp** *dscp*]

  No voice VLAN policy is configured by default.

- Configure the IP phone to transmit untagged frames. In this case, you can only manually add the interface to the voice VLAN.

  { **voice** | **voice-signaling** } **vlan untagged**

  No voice VLAN policy is configured by default.

(5) Configure the user interface to allow the advertisement of the Network Policy TLV.

a Return to the global configuration mode.

exit

b Enter the interface configuration mode.

interface *interface-type interface-number*

c Configure the interface to allow the advertisement of the Network Policy TLV.

lldp tlv-enable med-tlv network-policy profile *profile-num*

No network policy is configured by default.

1.19 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** commands to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

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

Table 1-7 Monitoring

Command	Purpose
clear lldp statistics [**interface** *interface-type interface-number*]	Clears LLDP statistics.
clear lldp table [**interface** *interface-type interface-number*]	Clears LLDP neighbor information.
show lldp local-information [**global** | **interface** interface-type interface-number]	Displays LLDP information on the local device, which will be organized as TLVs and sent to neighbors.
show lldp location { **civic-location | elin-location** } { **identifier** *id* **| interface** *interface-type interface-number* **| static** }	Displays the LLDP civic address or emergency telephone number of the local device.
show lldp neighbors [interface *interface-type interface-number*] [**detail**]	Displays the LLDP information of a neighbor.
show lldp network-policy { **profile** [*profile-num*] | **interface** *interface-type interface-number* }	Displays the LLDP network policy configuration of the local device.
show lldp statistics [**global | interface** *interface-type interface-number*]	Displays LLDP statistics.

Command	Purpose
show lldp status [**interface** *interface-type interface-number*]	Displays the LLDP status information.
show lldp tlv-config [**interface** *interface-type interface-number*]	Displays the configuration of TLVs to be advertised by an interface.
debug lldp error	Debugs LLDP error processing.
debug lldp event	Debugs LLDP event processing.
debug lldp ha	Debugs LLDP hot backup processing.
debug lldp packet	Debugs the LLDP packet receiving.
debug lldp stm	Debugs the LLDP state machine.

1.20 Configuration Examples

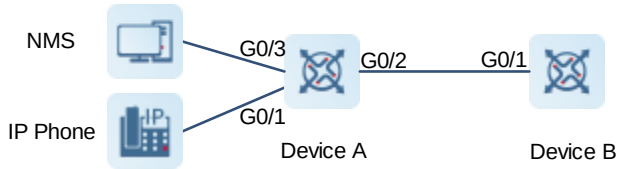
1.20.1 Checking the Neighbors Connected to the Device by Using the LLDP Function

1. Requirements

As shown in Figure 1-4, GigabitEthernet 0/1 of Device A is connected to the neighbor IP phone (MED device), and GigabitEthernet 0/2 is connected to the neighbor Device B. One NMS is connected to GigabitEthernet 0/3 of Device A. Check neighbor information on Device A by using the LLDP function.

2. Topology

Figure 1-4 Typical Topology of LLDP



3. Notes

- The LLDP function is enabled by default and no configuration is required.
- The default LLDP work mode of an interface is TxRx and no configuration is required.
- The default LLDP packet transmission interval is 30 seconds, the default LLDP packet transmission delay is 2 seconds, and no configuration is required.

4. Verification

Check information about the neighbor connected to port GigabitEthernet 0/2 of Device A. It can be seen that GigabitEthernet 0/2 `of Device A is connected to GigabitEthernet 0/1 of` Device B, and the neighbor supports the bridging (B) and routing (R) functions.

```
DeviceA# show lldp neighbors interface gigabitethernet 0/2
Capability codes:
   (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
   (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
System Name      Local Intf        Port ID         Capability       Aging-time
DeviceB         Gi0/2            Gi0/1           B, R            1minutes
49seconds

Total entries displayed: 1
```

Check details about the neighbor connected to GigabitEthernet 0/2 of Device A.

```
DeviceA# show lldp neighbors interface gigabitethernet 0/2 detail
------------------------------------------------------------------------------
LLDP neighbor-information of port [GigabitEthernet 0/2]
------------------------------------------------------------------------------
  Neighbor index                 : 1
  Device type                    : LLDP Device
  Update time                    : 18minutes 14seconds
  Aging time                     : 1minutes 44seconds

  Chassis ID type                : MAC address
  Chassis ID                     : 0074.9cee.f49e
  System name                    : DeviceB
  System description             : System description
  System capabilities supported   : Bridge, Router
  System capabilities enabled     : Bridge, Router

  Management address subtype      : ipv4
  Management address             : 172.26.147.182
  Interface numbering subtype     : ifIndex
  Interface number               : 8193
  Object identifier              :

  Management address subtype      : ipv6
  Management address             : 1010::1
  Interface numbering subtype     : ifIndex
  Interface number               : 4197
  Object identifier              :

  Port ID type                   : Interface name
  Port ID                        : Gi0/1
  Port description               :

  802.1 organizationally information
  Port VLAN ID                   : 101
  Port and protocol VLAN ID(PPVID)  : 0
     PPVID Supported             : NO
```

```
    PPVID Enabled                : NO
 VLAN name of VLAN 101            : VLAN0101
 Protocol Identity               :

 802.3 organizationally information
 Auto-negotiation supported       : YES
 Auto-negotiation enabled         : YES
 PMD auto-negotiation advertised   :
 Operational MAU type             : Speed(1000)/Duplex(Full)
 PoE support                     : NO
 Link aggregation supported       : YES
 Link aggregation enabled         : NO
 Aggregation port ID             : 0
 Maximum frame Size              : 1500
```

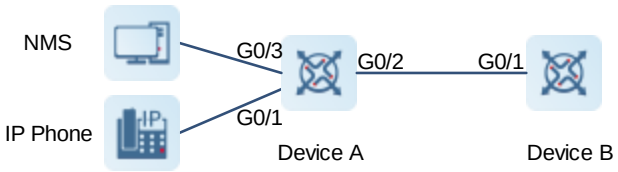
1.20.2 Configuring the LLDP Error Detection Function

1. Requirements

As shown in Figure 1-5, Device A and Device B are connected through Gigabit Ethernet (GE) interfaces. When an administrator configures the VLAN, port rate, duplex mode, aggregate port, and port MTU, an error will be prompted if the configurations do not match those on the connected neighbor.

2. Topology

Figure 1-5 Typical Topology of LLDP



3. Notes

- The LLDP function is enabled by default and no configuration is required.
- The default LLDP work mode of an interface is TxRx and no configuration is required.
- The LLDP error detection function is enabled by default and no configuration is required.
- The default LLDP packet transmission interval is 30 seconds, the default LLDP packet transmission delay is 2 seconds, and no configuration is required.

4. Verification

Forcibly set the rate of GigabitEthernet 0/2 of Device A to 100 Mbps. When the system prompts a mismatch with the rate and duplex mode of the connected port on the neighbor, the LLDP error detection function takes effect.

```
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# speed 100
```

```
%Warning: the speed/duplex of port GigabitEthernet 0/2 may not match with it's neighbor.
```

IP Service Configuration

1. ARP Configuration
2. IPv4 Basics Configuration
3. DHCP Configuration
4. DHCP Client Configuration
5. DHCP Snooping Configuration
6. DNS Configuration
7. IPv6 Basics Configuration
8. DHCPv6 Configuration
9. DHCPv6 Client Configuration
10. DHCPv6 Snooping Configuration
11. ND Snooping Configuration
12. TCP Configuration
13. IP REF Configuration

Contents

1 Configuring ARP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Basic Concepts 1
1.1.3 Principles 2
1.1.4 Protocols and Standards 5
1.2 Configuration Task Summary 5
1.3 Configuring a Static ARP Entry 6
1.3.1 Overview 6
1.3.2 Restrictions and Guidelines 6
1.3.3 Procedure 6
1.4 Configuring Dynamic ARP Learning Attributes 7
1.4.1 Overview 7
1.4.2 Configuration Tasks 7
1.4.3 Configuring the ARP Timeout Time 7
1.4.4 Configuring ARP Request Retransmission 8
1.4.5 Disabling Dynamic ARP Learning 8
1.4.6 Configuring Strict Dynamic ARP Learning 9
1.4.7 Configuring ARP Scanning 9
1.4.8 Configuring Scheduled Automatic ARP Scanning 10
1.5 Configuring ARP Entry Management 10
1.5.1 Overview 10

1.5.2 Configuration Tasks 11

1.5.3 Configuring a Limit on the Number of Unresolved ARP Entries 11

1.5.4 Configuring an ARP Learning Limit for an Interface 11

1.5.5 Configuring Fast ARP Entry Aging for an Interface 12

1.5.6 Configuring ARP Packet Rate Statistics Collection 12

1.5.7 Configuring the ARP Alarm Rate Limit 13

1.6 Enabling Trusted ARP 13

1.6.1 Overview 13

1.6.2 Procedure 13

1.7 Enabling Gratuitous ARP 14

1.7.1 Overview 14

1.7.2 Restrictions and Guidelines 14

1.7.3 Procedure 14

1.8 Enabling Proxy ARP 15

1.8.1 Overview 15

1.8.2 Restrictions and Guidelines 15

1.8.3 Procedure 15

1.9 Configuring Local Proxy ARP 15

1.9.1 Overview 15

1.9.2 Restrictions and Guidelines 15

1.9.3 Procedure 15

1.10 Configuring Any IP ARP 16

1.10.1 Overview 16

1.10.2 Restrictions and Guidelines 16

1.10.3 Procedure....16

1.11 Enabling ARP Trust Detection....17

1.11.1 Overview....17

1.11.2 Restrictions and Guidelines....17

1.11.3 Procedure....17

1.12 Enabling ARP-based IP Guard....18

1.12.1 Overview....18

1.12.2 Procedure....18

1.13 Configuring ARP Packet Filtering....18

1.13.1 Overview....18

1.13.2 Procedure....18

1.14 Restraining the Device from Sending ARP Requests to Authenticated VLANs....19

1.14.1 Overview....19

1.14.2 Restrictions and Guidelines....19

1.14.3 Procedure....19

1.15 Configuring Host Existence Judgment Prior to Proxy ARP Service....20

1.15.1 Overview....20

1.15.2 Restrictions and Guidelines....20

1.15.3 Procedure....20

1.16 Configuring ARP Entry Update During Active/Standby Switchover....20

1.16.1 Overview....20

1.16.2 Procedure....21

1.17 Sending ARP Requests to a Specific Sub VLAN....21

1.17.1 Overview....21

1.17.2 Procedure.....21

1.18 Monitoring 21

1.19 Configuration Examples.....23

1.19.1 Configuring Proxy ARP 23

1 Configuring ARP

1.1 Introduction

1.1.1 Overview

If two IP-enabled hosts need to communicate, a sender must learn the IP address and media access control (MAC) address of the receiver. With the MAC address, the sending host encapsulates IP datagrams into the data link layer (DLL) frames and transmits them over the physical network. The process of converting an IP address to a MAC address is called address resolution. There are two types of address resolution: Address Resolution Protocol (ARP) and proxy ARP.

ARP maps an IP address into a MAC address. The mappings of IP and MAC addresses are stored in the ARP cache of the network device.

1.1.2 Basic Concepts

1. ARP Messages

An ARP message can be an ARP request or ARP reply. The format of an ARP message is as follows:

Figure 1-1 ARP Message Format

<table>
<tr><td colspan="2">0 15 31</td></tr>
<tr><td colspan="2">Hardware type</td><td>Protocol type</td></tr>
<tr><td>Hardware length</td><td>Protocol length</td><td>OP</td></tr>
<tr><td colspan="3">Ethernet address of sender (0-31)</td></tr>
<tr><td colspan="2">Ethernet address of sender (31-47)</td><td>IP address of sender (0-15)</td></tr>
<tr><td colspan="2">IP address of sender (16-31)</td><td>Ethernet address of destination (0-15)</td></tr>
<tr><td colspan="3">Ethernet address of destination (16-47)</td></tr>
<tr><td colspan="3">IP address of destination</td></tr>
</table>

The description of fields in the ARP message is as follows:

- Hardware type: Indicates the type of a hardware address. For an Ethernet network, this value is **1**.
- Protocol type: Indicates the type of the protocol address to be mapped. For the IP protocol, this value is **0x0800**.
- Hardware length: Indicates the length of a hardware address, in bytes. For an Ethernet network, this value is **6**.
- Protocol length: Indicates the length of a protocol address, in bytes. For ARP requests or replies, this value is **4**.
- OP: Indicates the operation type. **1** indicates ARP requests, and **2** indicates ARP replies.
- Ethernet address of sender: Indicates a source MAC address, that is, the hardware address of a sender device.

- IP address of sender: Indicates a source IP address, that is, the IP address of a sender device.
- Ethernet address of destination: Indicates a destination MAC address, that is, the hardware address of a destination device. The value of this field is 0x00-00-00-00-00-00 for ARP requests.
- IP address of destination: Indicates a destination IP address, that is, the IP address of a destination device.

2. ARP Table

Each host maintains an ARP table that contains the mappings between IP addresses and MAC addresses. The mappings are called ARP entries.

Before sending an IP packet, a host first searches the ARP table for the MAC address corresponding to the destination IP address. If there is a corresponding MAC address in the ARP table, the host sends the IP packet directly to the MAC address instead of sending an ARP request message. If there is no corresponding MAC address in the ARP table, the host broadcasts an ARP request message to request the MAC address of the destination host. ARP entries can help greatly reduce the network traffic.

ARP entries can be classified as dynamic ARP entries or static ARP entries. The difference between them is as follows:

- Dynamic ARP entries are automatically generated and updated by the ARP protocol that exchanges ARP messages among devices, and will be aged and overwritten by new dynamic ARP entries.
- Static ARP entries are manually configured and maintained by the network administrator, and will not be aged or overwritten by dynamic ARP entries.

1.1.3 Principles

1. Static ARP Entries

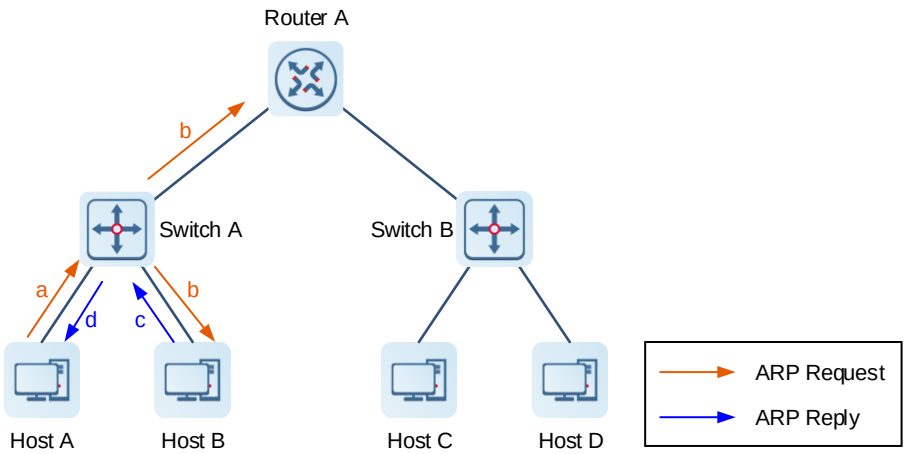
Static ARP entries are fixed mappings of IP and MAC addresses and they are created manually by the network administrator. The device cannot update the ARP entries. Static ARP entries can be deployed when communication security is a priority and network resources are sufficient.

2. Dynamic ARP Entries

Dynamic ARP allows devices to dynamically learn and update the mappings between IP and MAC addresses by exchanging ARP messages. Dynamic ARP entries can be deployed when real-time communication is priority or network resources are insufficient.

- **ARP implementation in the same network segment**

Figure 1-2 ARP Implementation in the Same Network Segment



As illustrated in Figure 1-2, host A has learned the IP address of host B and wants to send IP packets to host B. The address resolution process is as follows:

a Host A looks up in its ARP table and does not find the mapping between the IP and MAC addresses of host B. Host A then broadcasts an ARP request to request the MAC address of host B.

b After switch A receives the ARP request, switch A broadcasts the ARP request on the local network segment.

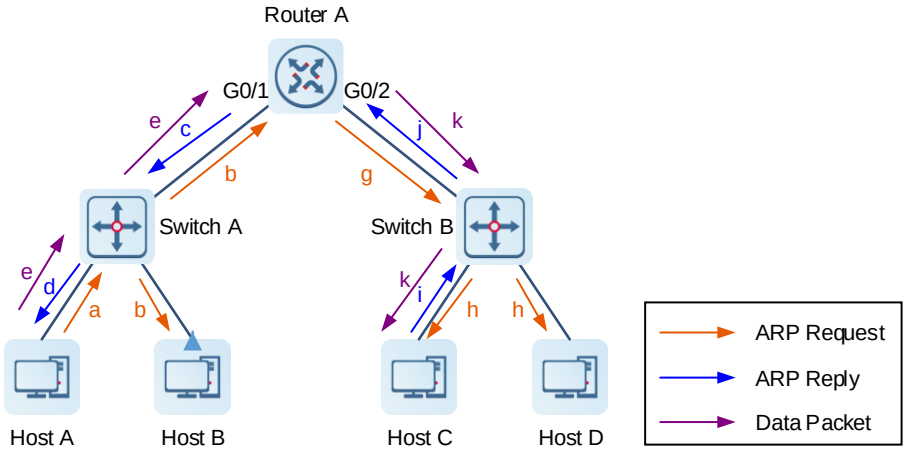
c After host B receives the ARP request, host B adds the MAC address of host A to its ARP table, and sends an ARP reply to host A. Since the destination IP address of the ARP request is not the IP address of router A, router A directly discards the ARP request after receiving it.

d Switch A forwards the ARP reply to the destination host A after receiving it.

e After host A receives the ARP reply, host A adds the MAC address of host B to its ARP table and sends the IP packets to host B.

- **ARP implementation in different network segments**

Figure 1-3 ARP Implementation in Different Network Segments



As illustrated in Figure 1-3, host A has learned the IP address of host C. For example, when host A sends an IP packet to host C, the address resolution process is as follows:

a Host A looks up in its ARP table and does not find the mapping between IP and MAC addresses of port GigabitEthernet 0/1 on the default gateway router A that is reachable to host C. Host A then sends an ARP broadcast request to request the MAC address of port GigabitEthernet 0/1 of router A.

f After receiving the ARP request, switch A broadcasts the packet on the local network segment.

g After receiving the ARP request, router A adds the MAC address of host A into its ARP table, and sends an ARP reply to host A. Since the destination IP address of the ARP request is not the IP address of host B, host B directly discards the ARP request after receiving it.

h Switch A forwards the ARP reply to the destination host A after receiving it.

i After receiving the ARP reply, host A adds the MAC address of port GigabitEthernet 0/1 of router A into its ARP table and sends the IP packet to router A.

j Router A looks up in the routing table and sends the IP packet from port GigabitEthernet 0/1 to port GigabitEthernet 0/2.

k Router A looks up in its ARP table and finds that there is no MAC address of host C. Router A then sends an ARP broadcast request to request the MAC address of host C.

l After switch B receives the ARP request, switch B broadcasts the packet on the local network segment.

m After host C receives the ARP request, host C adds the MAC address of port GigabitEthernet 0/2 of router A into its ARP table, and sends an ARP reply to router A. Since the destination IP address of the ARP request is not the IP address of host D, host D directly discards the ARP request after receiving it.

n Switch B forwards the ARP reply to the destination router A after receiving it.

o After router A receives the ARP reply, router A adds the MAC address of host C into its ARP table and sends the IP packet to host C.

3. Trusted ARP

When a user goes online on a GPRS support node (GSN) client, the authentication server obtains the user's real the mapping between IP and MAC addresses through the access switch, and adds trusted ARP entries on the user's gateway switch. This process is transparent to network administrators and does not require their extra work.

Trusted ARP entries have characteristics of both static and dynamic ARP entries, with a priority higher than that of dynamic ARP entries and lower than that of static ARP entries. Trusted ARP entries have an aging mechanism similar to that of dynamic ARP entries. When an ARP entry ages, the device actively sends an ARP request to detect whether the peer host exists. If the host sends a reply, the device regards the host active and updates the aging time of the ARP entry. Otherwise, the device deletes the ARP entry. Trusted ARP entries have characteristics of static ARP entries. The device cannot dynamically update information about the MAC addresses and interfaces in the trusted ARP entries by learning ARP messages.

Since trusted ARP entries come from authentic sources and will not be updated, they can efficiently prevent ARP spoofing targeting the gateway.

4. Gratuitous ARP

A gratuitous ARP message is a special ARP message. In a gratuitous ARP message, both the source and the destination IP addresses carried are the IP address of the local device.

Gratuitous ARP packets have the following purposes:

- Detecting IP address conflict If the device receives a gratuitous ARP packet and finds that the IP address in the packet is the same as its own IP address, it sends an ARP reply to notify the peer of the IP address conflict.
- Sending a gratuitous ARP packet to notify other devices to update ARP entries when the interface MAC address of a device changes. For example, in dual-node hot standby mode, when services are switched from the master device to the slave device, the MAC address of the previously slave device in the ARP entries on the connected device needs to be updated as that of the current master device. Generally, when services are switched from the master device to the slave device, the new master device after switchover sends a gratuitous ARP request to the network to notify other devices to update their ARP entries.
- Updating ARP entries based on gratuitous packets After receiving a gratuitous ARP message, the device checks whether a dynamic ARP entry corresponding to the source IP address in the gratuitous ARP packet exists. If yes, the device updates the ARP entry based on the information carried in the gratuitous ARP packet.

5. Proxy ARP

Proxy ARP allows devices on different subnets to resolve IP addresses into MAC addresses. If a device receives an ARP request whose source IP address is on a different network segment from the destination IP address and knows the route to the destination IP address, the device sends an ARP reply containing its own MAC address.

6. Local Proxy ARP

Local proxy ARP means that a device acts as a proxy ARP in the same virtual local area network (VLAN) that can be a common VLAN or sub VLAN.

After local proxy ARP is enabled on a device, the device can help hosts obtain the MAC addresses of other hosts in the VLAN. When port protection is enabled on the device, hosts connected to different ports are isolated at Layer 2. After receiving an ARP request, the device with local proxy ARP enabled serves as a proxy to send an ARP reply with its own Ethernet MAC address. In this case, hosts communicate with each other through Layer 3 routes.

7. Any IP ARP

Any IP ARP allows a device to access the network with any IP address. For example, a user is using a laptop in a hotel and wants to access the Internet without changing the configured IP address and gateway. After the gateway receives an ARP request and finds that the source IP address of the sender is in a different subnet and the destination address may not be its own address, the gateway still sends an ARP reply, with the MAC address of the gateway's Ethernet MAC address, and creates a direct route for the host.

1.1.4 Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol
- RFC 1027: Using ARP to implement transparent subnet gateways

1.2 Configuration Task Summary

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring a Static ARP Entry
- Configuring Dynamic ARP Learning Attributes
- Configuring ARP Entry Management
- Enabling Trusted ARP
- Enabling Gratuitous ARP
- Enabling Proxy ARP
- Configuring Local Proxy ARP
- Configuring Any IP ARP
- Configuring other advanced ARP functions
  - Enabling ARP Trust Detection
  - Enabling ARP-based IP Guard
  - Configuring ARP Packet Filtering
  - Restraining the Device from Sending ARP Requests to Authenticated VLANs
  - Configuring Host Existence Judgment Prior to Proxy ARP Service
  - Configuring ARP Entry Update During Active/Standby Switchover
  - Sending ARP Requests to a Specific Sub VLAN

1.3 Configuring a Static ARP Entry

1.3.1 Overview

Users can manually configure static ARP entries to prevent the device from learning incorrect ARP entries, thus affecting the network connectivity.

1.3.2 Restrictions and Guidelines

After a static ARP entry is configured on an Layer 3 switch, the Layer 3 switch performs routing only after learning the physical port corresponding to MAC address carried in the static ARP entry.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static ARP entry.

arp [**vrf** *vrf-name* | **oob** [*mgmt-name*]] *ip-address mac-address arp-type*

No static ARP entry is configured by default.

1.4 Configuring Dynamic ARP Learning Attributes

1.4.1 Overview

The dynamic ARP learning function is enabled by default. You can configure ARP learning attributes as needed, for example, specify ARP entry timeout time, the number of times and interval that an ARP request can be transmitted consecutively, strict dynamic ARP learning function, ARP scanning, and scheduled automatic ARP scanning.

1.4.2 Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring the ARP Timeout Time
- Configuring ARP Request Retransmission
- Disabling Dynamic ARP Learning
- Configuring Strict Dynamic ARP Learning
- Configuring ARP Scanning
- Configuring Scheduled Automatic ARP Scanning

1.4.3 Configuring the ARP Timeout Time

1. Overview

Before an ARP entry times out, the device sends a unicast ARP request to detect whether the peer is online. If the device receives an ARP reply from the peer, it means that the peer is still online and the ARP entry is reserved. Otherwise, this ARP entry will be deleted. The ARP timeout time can be set as required.

2. Restrictions and Guidelines

The ARP timeout configuration only applies to dynamic mappings between IP and MAC addresses. When the ARP timeout time is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth. In general, the ARP timeout time does not need to be set.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the ARP timeout time.

arp timeout *time*

The default timeout time of dynamic ARP entries in the ARP cache is **3600** seconds.

1.4.4 Configuring ARP Request Retransmission

1. Overview

The device sends a certain number of ARP requests at a certain time interval during address resolution until the device receives an ARP reply. This function is used to configure the interval and number of times that an ARP request can be transmitted consecutively.

2. Restrictions and Guidelines

The shorter the retransmission interval is, the faster the resolution is. The more times the ARP request can be transmitted consecutively, the more likely the resolution will succeed and the more bandwidth ARP will be consumed.

If the network resources are insufficient, you are advised to set the ARP request retransmission interval to a larger value and the number of retransmission times to a smaller value, to reduce bandwidth consumption.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the ARP request retransmission interval.

arp retry interval *interval*

The default ARP request retransmission interval is 1 second.

(5) Configure the number of times that an ARP request can be transmitted consecutively.

arp retry times *times*

The default number of times that an ARP request can be transmitted consecutively is 5. That is, if no ARP reply packet is received, the ARP request packet will be retransmitted for four consecutive times.

1.4.5 Disabling Dynamic ARP Learning

1. Overview

The dynamic ARP learning function can be disabled on an interface. Then, the interface will not perform dynamic ARP learning.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Disable dynamic ARP learning.

no arp-learning enable

The ARP learning function is enabled by default.

1.4.6 Configuring Strict Dynamic ARP Learning

1. Overview

After this function is enabled on a device, only the ARP replies in response to the ARP requests actively sent by the device can trigger the device to learn ARP entries.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable strict dynamic ARP learning.

arp strict-learning enable

Strict dynamic ARP learning is disabled by default.

1.4.7 Configuring ARP Scanning

1. Overview

This function is usually used together with the Web-based dynamic-to-static ARP entry conversion function. After ARP scanning is enabled on an interface, the device scans neighbors in the specified range and learns the ARP entries of these neighbors.

2. Restrictions and Guidelines

The device can scan the neighbors in the network segments, to which the primary IP address and secondary IP addresses belong, on an interface or scans only the neighbors in the specified address range. ARP scanning takes effect once after it is configured, and can be executed when the Layer 3 interface is up (that is, the link is up and an IP address is configured for the interface). However, ARP scanning configuration cannot be saved and will lose effect the next time.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable ARP scanning.

arp scan [*start-ip-address end-ip-address*]

ARP scanning is disabled by default.

1.4.8 Configuring Scheduled Automatic ARP Scanning

1. Overview

After scheduled automatic ARP scanning is enabled on an interface, the device scans neighbors in the specified range and learns the ARP entries of these neighbors. If ARP entries are not learned from neighbors, after the current scanning ends, the device waits for the scanning interval (5 minutes by default) and then starts next scanning until the entries are learned.

2. Restrictions and Guidelines

- Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.
- The scanning interval ranges from 1 to 30, in minutes.
- The scanning rate ranges from 1 to 100, in IP addresses per second.
- Up to 30 instances can be configured.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable scheduled automatic ARP scanning.

arp scan auto [*start-ip-address end-ip-address*]

The scheduled automatic ARP scanning function is disabled by default.

(5) (Optional) Configure the scheduled automatic ARP scanning interval.

arp scan interval *time*

The default interval of scheduled automatic ARP scanning is 5 minutes.

(6) (Optional) Configure the scheduled automatic ARP scanning rate.

arp scan rate *rate-value*

The default scheduled automatic ARP scanning rate is **20** IP addresses per second.

1.5 Configuring ARP Entry Management

1.5.1 Overview

Entries in the ARP cache can be managed as required, such as limiting the capacity of ARP entries and configuring fast aging of ARP entries.

1.5.2 Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring a Limit on the Number of Unresolved ARP Entries
- Configuring an ARP Learning Limit for an Interface
- Configuring Fast ARP Entry Aging for an Interface
- Configuring ARP Packet Rate Statistics Collection
- Configuring the ARP Alarm Rate Limit

1.5.3 Configuring a Limit on the Number of Unresolved ARP Entries

1. Overview

In a local area network (LAN), ARP attacks and scanning may cause a large number of unresolved ARP entries generated on the gateway. As a result, the gateway fails to learn the MAC addresses of the hosts. To prevent this situation, if a large number of unresolved entries exist in the ARP cache and remain in the table after a while, you are advised to use this command to limit the number of unresolved ARP entries.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a limit on the number of unresolved ARP entries.

arp unresolve *unresolved-number*

The maximum number of unresolved ARP entries that can be held in an ARP cache is the total capacity of ARP entries by default.

1.5.4 Configuring an ARP Learning Limit for an Interface

1. Overview

Limiting the number of ARP entries that can be learned by an interface can flexibly control the on-demand assignment of ARP entry resources, to prevent resource waste. In addition, this can prevent malicious ARP attacks. When the device is attacked maliciously and the ARP entry learning number is not limited, the device will generate a large number of ARP entries, which occupy excessive entry resources.

2. Restrictions and Guidelines

The configured value must be equal to or greater than the number of the ARP entries learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ARP entry capacity supported by the device.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an ARP learning limit for the interface.

arp cache interface-limit *limit*

The number of ARP entries that can be learned by an interface is not limited by default.

1.5.5 Configuring Fast ARP Entry Aging for an Interface

1. Overview

If a host goes offline or encounters an abnormal condition, the device fails to learn the ARP entry. When the MAC address corresponding to the ARP entry ages, the dynamic ARP entry starts aging one hour after the aging time by default. If this feature is enabled on an interface, after the MAC address ages, the dynamic ARP entry ages rapidly to realize fast route convergence of the host.

2. Restrictions and Guidelines

- This function can be configured only on SVIs.
- When the conversion of ARP entries into host routes is enabled on the device, you are advised to also enable this function to help achieve fast route convergence.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable fast ARP entry aging.

arp fast-aging enable

The fast ARP entry aging function is disabled by default.

1.5.6 Configuring ARP Packet Rate Statistics Collection

1. Overview

After this function is enabled, the device collects statistics on ARP messages received by each interface in a fixed period of time by replies, requests, and unknown packets.

2. Restrictions and Guidelines

The default statistics collection interval is 5 seconds. If there are many interfaces and the rate is not as expected, appropriately adjust the statistics collection interval. The minimum statistics collection interval can be set to 1 second.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable ARP packet rate statistics collection.

arp rate-statistic enable

The ARP packet rate statistics collection is disabled by default.

(4) (Optional) Configure the interval for ARP packet rate statistics collection.

arp rate-statistic compute interval *interval*

The default interval for collecting ARP packet rate statistics is 5 seconds.

1.5.7 Configuring the ARP Alarm Rate Limit

1. Overview

You can configure the ARP alarm rate limit to adjust the printing rate of ARP syslog alarms.

2. Restrictions and Guidelines

The actual ARP alarm rate may be lower than the configured rate, depending on system performance.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the ARP alarm rate limit.

arp warning-limit interval *interval* **times** *time*

The default ARP alarm rate limit interval is 50 seconds and the default upper limit of alarms allowed within this interval is 10.

1.6 Enabling Trusted ARP

1.6.1 Overview

Since trusted ARP entries come from authentic sources and will not be updated, they can efficiently prevent ARP spoofing targeting the gateway.

1.6.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable trusted ARP.

service trustedarp

Trusted ARP is disabled by default.

(4) (Optional) Enable VLAN translation when a trusted ARP entry is added.

arp trusted user-vlan *vlan-id* **translated-vlan** *vlan-id*

The VLAN translation is disabled when a trusted ARP entry is added by default.

Configure this command only when the VLAN delivered by the server differs from the valid VLAN in the trusted ARP entry.

(5) (Optional) Enable trusted ARP aging.

arp trusted aging

Trusted ARP entries are not aged by default.

After you configure this command, trusted ARP entries begin to age, and the aging time is the same as that of dynamic ARP entries. You can run the **arp timeout** command in interface configuration mode to set the aging time.

(6) (Optional) Adjust the capacity of trusted ARP entries.

arp trusted *number*

The maximum number of trusted ARP entries is half of the capacity of the ARP table by default.

Trusted ARP entries and other entries share the memory. If trusted ARP entries occupy much space, dynamic ARP entries may not have sufficient space. Set the capacity based on the actual requirement. Do not set it to an excessively large value.

1.7 Enabling Gratuitous ARP

1.7.1 Overview

Gratuitous ARP packets are special ARP messages. In a gratuitous ARP message, the source and destination IP addresses are the IP address of the local device. This function enables an interface to periodically send gratuitous ARP packets.

1.7.2 Restrictions and Guidelines

Generally, you need to enable this function on an interface that serves as the gateway of downlink devices so that the MAC address of the gateway of the downlink devices are updated periodically to prevent others from faking the gateway.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the function of sending gratuitous ARP requests.

arp gratuitous-send enable

The function of sending gratuitous ARP requests is enabled by default.

(5) Configure the interval for sending gratuitous ARP requests.

arp gratuitous-send interval *interval* [*number*]

The function of sending gratuitous ARP requests at intervals is disabled by default.

1.8 Enabling Proxy ARP

1.8.1 Overview

The device acts as a proxy to reply to ARP requests from other hosts. If a device receiving an ARP request finds the source IP address in a different network from the destination IP address and knows the route to the destination address, the device sends an ARP reply containing its own Ethernet MAC address.

1.8.2 Restrictions and Guidelines

By default, proxy ARP is disabled on Layer 3 switches.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enables proxy ARP.

ip proxy-arp

Proxy ARP is disabled by default.

1.9 Configuring Local Proxy ARP

1.9.1 Overview

After local proxy ARP is enabled, the device can help hosts obtain the MAC addresses of other hosts in the same subnet.

1.9.2 Restrictions and Guidelines

This function can be configured only on SVIs.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enables local proxy ARP.

local-proxy-arp

Local proxy ARP is disabled by default.

1.10 Configuring Any IP ARP

1.10.1 Overview

Users can access the network with any IP address. This applies when a user uses a laptop in a hotel and wants to access the Internet without changing the configured IP address and gateway.

1.10.2 Restrictions and Guidelines

This function is not applicable in the following two scenarios, in which a user must modify the configuration before accessing the Internet.

- The user's IP address is in the same network segment as the interface directly connected to the device. However, the configured gateway IP address is not the IP address configured for the interface directly connected to the device.
- The user's IP address is not in the same network segment as the interface directly connected to the device, but in the network segment of another interface. That means an IP address conflict occurs.

  As the user's IP address is not in the same network segment as the interface directly connected to the device, the dynamic ARP entry and direct route are generated only when the user initiates an ARP request. Therefore, in some scenarios (including but not limited to the following ones), the user will not be able to access the Internet unless the ARP entry is cleared and the gateway address is relearned on the user host.

  - The device acts as a proxy to respond to ARP requests. After the user host learns the MAC address of the device, the administrator deletes the dynamic ARP entry on the device. As a result, the user's dynamic ARP entry and direct route are removed and the user cannot receive the reply.
  - The device acts as a proxy to respond to ARP requests. After the user host learns the MAC address of the device, if any IP ARP is disabled and then enabled again on the interface, the user cannot receive the reply The cause is that the user's dynamic ARP entry and direct route are immediately deleted when the any IP ARP function is disabled on the interface.

Caution

If static ARP entries or the ARP entries involving the Virtual Router Redundancy Protocol (VRRP) IP addresses exist, dynamic ARP entries generated by any IP ARP will be overwritten or fail to be added, and any IP ARP does not take effect.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable any IP ARP.

arp any-ip

The any IP ARP function is disabled by default.

1.11 Enabling ARP Trust Detection

1.11.1 Overview

ARP trust detection is used to prevent excessive useless ARP entries generated due to ARP spoofing from occupying device resources. After ARP trust detection is enabled on an Layer 3 interface and the device receives an ARP request from this interface:

(2) If the corresponding entry does not exist, the device creates a dynamic ARP entry and performs neighbor unreachability detection (NUD) after 1 to 5 seconds. That is, the device ages the newly learned ARP entry and sends a unicast ARP request. If the device receives an ARP update packet from the peer within the aging time, it stores the entry. Otherwise, it deletes the entry.

(3) If the corresponding ARP entry exists, the device does not perform NUD.

(4) If the MAC address in the existing dynamic ARP entry is updated, the device performs NUD.

1.11.2 Restrictions and Guidelines

- Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.
- After this function is disabled, the device no longer performs NUD for learning or updating ARP entries.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable ARP trust detection.

arp trust-monitor enable

ARP trust detection is disabled by default.

1.12 Enabling ARP-based IP Guard

1.12.1 Overview

When receiving unresolved IP packets, the device cannot forward them through the hardware but sends them to the CPU for address resolution, that is, ARP learning. If a large number of such packets are sent to the CPU, the CPU will be congested, affecting other services on the device.

After ARP-based IP guard is enabled, the device will count the number of received ARP packets based on the destination IP address. When the number of packets with the same destination IP address exceeds a certain threshold, the device deems it as a CPU attack and will send a drop entry to the hardware so that the hardware will not send subsequent ARP packets with this destination IP address to the CPU. After the address resolution is complete, the device updates the entry to the forwarding state and continues to forward the packets with this destination IP address.

1.12.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable ARP-based IP guard.

arp anti-ip-attack *attack-num*

The default number of IP packets for triggering the discarding of ARP entries is 3.

1.13 Configuring ARP Packet Filtering

1.13.1 Overview

- ARP packet filtering supports the following functions:
  Filters out received gratuitous APR packets.
- Filters out ARP packets that hit ACL rules.
- Filters out ARP packets whose source MAC addresses is not consistent with the Ethernet source MAC address.
- Filters out ARP packets whose destination MAC addresses is not consistent with the Ethernet destination MAC address.

1.13.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure ARP packet filtering. Perform at least one of the following configuration steps:

- Enable gratuitous ARP filtering.

arp filter gratuitous

Gratuitous ARP filtering is disabled by default.

- Enable ARP-based ACL filtering.

  arp filter acl *acl-number*

  ARP-based ACL filtering is disabled by default.

- Enables the function of checking the source MAC addresses of ARP packets.

  arp filter smac-illegal

  The function of checking the source MAC addresses of ARP packets is disabled by default.

- Enable the function of checking the destination MAC addresses of ARP packets.

  arp filter dmac-illegal

  The function of checking the destination MAC addresses of ARP packets is disabled by default.

1.14 Restraining the Device from Sending ARP Requests to Authenticated VLANs

1.14.1 Overview

In gateway authentication mode, all sub VLANs in a super VLAN are authenticated VLANs by default. Users in an authenticated VLAN have to pass authentication to access the network. After authentication, a static ARP entry is generated on the device. Therefore, when accessing an authenticated user, the device does not need to send ARP requests to the authenticated VLAN. If the device attempts to access users in an authentication-exempt VLAN, it only needs to send ARP requests to the authentication-exempt VLAN.

1.14.2 Restrictions and Guidelines

- This function can be configured only on SVIs.
- In gateway authentication mode, the device does not send ARP requests to the authenticated VLANs by default. If the device needs to access authentication-exempt users in an authenticated VLAN, disable this function.

1.14.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the device not to send ARP requests to authenticated VLANs.

arp suppress-auth-vlan-req

ARP requests are not sent to authenticated VLANs by default.

1.15 Configuring Host Existence Judgment Prior to Proxy ARP Service

1.15.1 Overview

When two devices form a VRRP network and local proxy ARP is enabled on them, if the slave VRRP device sends an ARP request to a terminal, the master VRRP device will act as a proxy of the terminal and send an ARP reply to the slave VRRP device regardless of whether the terminal exists. As a result, the slave VRRP device learns a large number of proxy ARP entries.

After the host existence judgment prior to proxy ARP service is enabled, the master VRRP device, upon receiving an ARP request, first judges whether the ARP entry corresponding to the destination IP address exists. If yes, the master VRRP device acts as a proxy ARP. If no, the master VRRP device does not act as a proxy ARP. In addition, the gateway automatically broadcasts an ARP request for the ARP entry corresponding to the destination IP address. This prevents the case that the gateway fails to act as a proxy to respond to an ARP request of the destination ARP address if it does not have an ARP entry corresponding to the destination IP address.

After the host existence judgment prior to proxy ARP service is disabled, if the proxy conditions are met, the master ARP device directly acts as a proxy upon receiving an ARP request, without judging whether the ARP entry corresponding to the destination IP address has been resolved.

1.15.2 Restrictions and Guidelines

The **arp proxy-resolved** command is enabled on devices by default. That is, the master VRRP device responds to an ARP request as a proxy only after the destination IP address has been resolved.

1.15.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the master VRRP device to forcibly respond to ARP requests as a proxy.

no arp proxy-resolved

By default, the master VRRP device judges the existence of the ARP entry corresponding to a destination IP address before the device responds to an ARP request as a proxy ARP.

1.16 Configuring ARP Entry Update During Active/Standby Switchover

1.16.1 Overview

This function can be enabled to quickly update ARP entries of a downlink device after VSU active/standby switchover, especially when the downlink device is similar to a server with dual network interface cards. When the slave device becomes the master, it will actively send ARP requests to SVIs (that are not in a super VLAN) of up to 1000 downlink terminals. After the terminals reply to these ARP requests, the device can update the ARP and MAC tables.

1.16.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of actively sending ARP requests to SVIs of downlink terminals during active/standby switchover.

arp switch-over resolve

ARP requests are not actively sent to downlink terminals during VSU active/standby switchover by default.

1.17 Sending ARP Requests to a Specific Sub VLAN

1.17.1 Overview

In a super VLAN scenario, the device actively broadcasts ARP resolution requests to the entire super VLAN by default. If there are many sub VLANs in the super VLAN, the ARP messages will be replicated in large quantities, which will affect device performance.

Most terminals (such as PCs and servers) request ARP information of the gateway before accessing the network. Therefore, there is no need to actively broadcast ARP resolution requests to the sub VLANs where these terminals reside. For dumb terminals (that do not actively send gratuitous ARP packets), this command can be deployed in a specified *vlan-list* to enable the device to actively send ARP resolution requests to these VLANs.

1.17.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable ARP to actively broadcast resolution requests to a specific sub VLAN in a super VLAN.

arp resolve vlan { *vlan-list* | **none** }

ARP does not actively broadcast resolution requests to a specific sub VLAN in a super VLAN by default.

1.18 Monitoring

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

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** command to clear information.

Caution

Inappropriate use of the **clear** command may lose vital information and thus interrupt services.

Table 1-1 Monitoring

Command	Purpose
show arp trusted [*ip-address* [*mask*]]	Displays trusted ARP entries.
clear arp-cache trusted [*ip-address* [*mask*]]	Clears trusted ARP entries.
clear arp-cache [[**vrf** *vrf-name* | **oob**] [*ip-address* [*mask*]] | [**interface** *interface-type interface-number*]]	Clears dynamic ARP entries.
clear arp-cache packet statistics [*interface-type interface-number*]	Clears ARP packet statistics.
show arp [**detail**] [*interface-type interface-number* | [**vrf** *vrf-name*] [*ip-address* [*mask*] | *mac-address* | **static** | **complete** | **incomplete**] | **subvlan** { *subvlan-number* | **min-max** *min-value max-value* }]	Displays the ARP table.
show arp oob [*ip-address* [*mask*] | **static** | **complete** | **incomplete** | *mac-address*]	Displays the ARP table on the management interface.
show ip arp [**vrf** *vrf-name*]	Displays the ARP table.
show arp [**detail**] **trusted** [*ip-address* [mask]]	Displays the trusted ARP table.
show arp counter	Displays the count of ARP entries.
show arp timeout	Displays the aging time of dynamic ARP entries.
show arp packet statistics [*interface-type interface-number*]	Displays ARP packet statistics.
show arp rate-statistic [*interface-type interface-number*]	Displays ARP packet rate statistics.
show arp timeout	Displays the aging time of dynamic ARP entries.
show arp flapping record	Displays ARP flapping records.
show arp anti-attack statistics	Displays the statistics on illegal ARP packets.
show arp dynamic-entry-limit	Displays the statistics on the ARP capacity limit of a line card.

debug arp	Displays the statistics on ARP packets sent and received.
debug arp event	Displays the creation and deletion status of ARP entries.

1.19 Configuration Examples

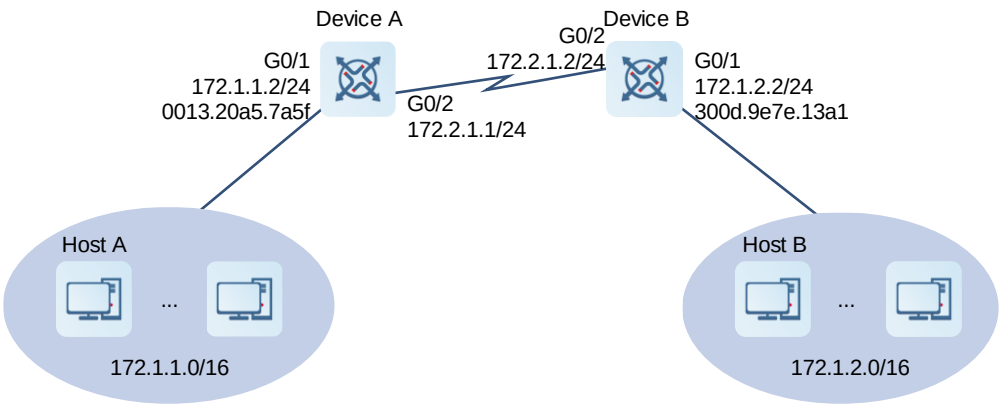
1.19.1 Configuring Proxy ARP

1. Requirements

As shown in Figure 1-4, the IP addresses of host A and host B are on the same network segment, but are isolated in two LANs by routers. Neither of the two hosts is configured with a default gateway, and the two routers are connected over a serial link. Enable proxy ARP on the routers to achieve direct communication between hosts in different LANs.

2. Topology

Figure 1-4 Topology of Proxy ARP



3. Notes

- Enable proxy ARP on interfaces of device A and device B that are connected to hosts.
- Configure default routes on device A and device B.

4. Procedure

(1) Configure device A.

Configure an IP address for port GigabitEthernet 0/1.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 172.1.1.2 24
```

Enable proxy ARP on port GigabitEthernet 0/1.

```
DeviceA(config-if-GigabitEthernet 0/1)# ip proxy-arp
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Configure an IP address for port GigabitEthernet 0/2.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ip address 172.2.1.1 24
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

Configure the static route to 172.1.2.0/16.

```
DeviceA(config)# ip route 172.1.2.0 255.255.0.0 gigabitethernet 0/2
```

(2) Configure device B.

Configure an IP address for port GigabitEthernet 0/1.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 172.1.2.2 24
```

Enable proxy ARP on port GigabitEthernet 0/1.

```
DeviceB(config-if-GigabitEthernet 0/1)# ip proxy-arp
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure an IP address for port GigabitEthernet 0/2.

```
DeviceB(config)# interface gigabitethernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# ip address 172.2.1.2 24
DeviceB(config-if-GigabitEthernet 0/2)# exit
```

Configure the static route to 172.1.1.0/16.

```
DeviceB(config)# ip route 172.1.1.0 255.255.0.0 gigabitethernet 0/2
```

(3) Configure hosts.

Set the IP address of host A to 10.0.1.1/24.

Set the IP address of host B to 10.0.2.1/24.

5. Verification

Host A can ping host B successfully.

You can check the ARP table of host A and find that the MAC address corresponding to host B is the MAC address of port GigabitEthernet 0/1 on device A.

6. Configuration Files

- Device A configuration file

```
!
hostname DeviceA
ip route 172.1.2.0 255.255.0.0 gigabitethernet 0/2
!
 interface gigabitethernet 0/1
 ip address 172.1.1.2 24
 ip proxy-arp
!
 interface gigabitethernet 0/2
 ip address 172.2.1.1 24
```

```
!
```

- Device B configuration file

```
!
hostname DeviceB
ip route 172.1.1.0 255.255.0.0 gigabitethernet 0/2
!
 interface gigabitethernet 0/1
 ip address 172.1.2.2 24
 ip proxy-arp
!
 interface gigabitethernet 0/2
 ip address 172.2.1.2 24
!
```

Contents

1 Configuring IPv4 Basics 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Basic Concepts 1
1.1.3 Principles 4
1.1.4 Protocols and Standards 7
1.2 Configuration Task Summary 7
1.3 Configuring an IP Address for an Interface 8
1.3.1 Overview 8
1.3.2 Configuration Tasks 8
1.3.3 Configuring a Static IP Address for an Interface 8
1.3.4 Configuring an Unnumbered Interface to Borrow an IP Address 8
1.3.5 Configuring an IP Address Combination for an Interface 9
1.3.6 Configuring an IP Broadcast Address 10
1.4 Configuring the Default Gateway for a Management Interface 10
1.4.1 Overview 10
1.4.2 Restrictions and Guidelines 10
1.4.3 Procedure 10
1.5 Configuring Directed Broadcast Packets 10
1.5.1 Overview 10
1.5.2 Restrictions and Guidelines 11
1.5.3 Procedure 11

1.6 Configuring ICMP Messages 11

1.6.1 Overview 11

1.6.2 Configuration Tasks 11

1.6.3 Enabling the Function of Sending TTL Timeout Messages 11

1.6.4 Enabling the Timestamp Query 12

1.6.5 Enabling the Function of Sending ICMP Destination Unreachable Messages 12

1.6.6 Enabling the Function of Sending ICMP Redirection Messages 12

1.6.7 Enabling the Function of Sending ICMP Mask Reply Messages 12

1.7 Configuring the Transmission Rate of ICMP Error Messages 13

1.7.1 Overview 13

1.7.2 Restrictions and Guidelines 13

1.7.3 Procedure 13

1.8 Setting the IP MTU Value 14

1.8.1 Overview 14

1.8.2 Restrictions and Guidelines 14

1.8.3 Procedure 14

1.9 Setting the IP TTL Value 14

1.9.1 Overview 14

1.9.2 Procedure 14

1.10 Configuring IP Routed Port Protection 15

1.10.1 Overview 15

1.10.2 Restrictions and Guidelines 15

1.10.3 Procedure 15

1.11 Configuring the IP Source Route Option 15

1.11.1 Overview 15

1.11.2 Restrictions and Guidelines 15

1.11.3 Procedure 15

1.12 Monitoring 16

1.13 Configuration Examples 16

1.13.1 Configuring IPv4 Addresses for Network Communication 16

1 Configuring IPv4 Basics

1.1 Introduction

1.1.1 Overview

Internet Protocol (IP) is one of the most core protocols in the Transmission Control Protocol (TCP)/IP protocol suite and works at the network layer. Each IP device in the network needs a logical virtual address, which is used by the IP protocol to realize communication between devices. This address is usually called IP address.

The Internet Protocol version 4 (IPv4) is the fourth revision of the Internet Protocol, and is also the first version that has been widely used. The Internet Protocol version 6 (IPv6), the successor of IPv4, is still in its early stage of deployment in 2011 when IPv4 addresses were about to be used up. IPv4 uses the 32-bit address format, so there are only 4,294,967,296 addresses in the address space, some of which are reserved for special purposes.

Note

The following description is for IPv4 only, and IP addresses mentioned in this document refer to IPv4 addresses.

1.1.2 Basic Concepts

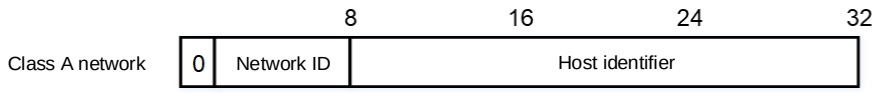
1. Classification of IP Addresses

IP addresses are used for interconnection at the IP layer. An IP address consists of 32 bits in binary. To facilitate writing and description, an IP address is generally expressed in decimal notation. When expressed in decimal notation, an IP address is divided into four groups, with eight bits in each group. The value range of each group is from 0 to 255, and groups are separated by dots (.), which are called dotted decimal notation. For example, "192.168.1.1" is an IP address expressed in decimal notation.

A 32-bit IP address consists of two parts: network ID and local address. A network ID indicates a network identifier, and a local address identifies a host. Based on the values of the first several bits in the network part, IP addresses in use can be classified into four classes.

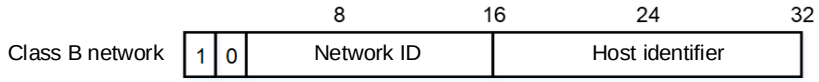
- For a class A address, the most significant bit is "0", the following 7 bits indicate a network ID, and the last 24 bits indicate a local address (host identifier). There are 2^7 = 128 class A networks in total.

Figure 1-1 Class A Network



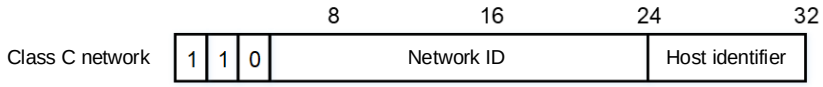
- For a class B address, the two most significant bits are "10", the following 14 bits indicate a network ID (network identifier), and the last 16 bits indicate a local address (host identifier). There are 2^{14}=16,384 class B networks in total.

Figure 1-2 Class B Network



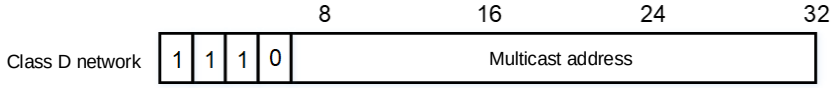
- For a class C address, the three most significant bits are "110", and the following 21 bits indicate a network ID, and the last 8 bits indicate a local address. There are 2^{21}=2,097,152 class C networks in total.

Figure 1-3 Class C Network



- For a class D address, the four most significant bits are "1110" and other bits are designated for multicast addresses.

Figure 1-4 Class D Network



Note

The addresses with the four most significant bits of "1111" cannot be assigned. These addresses are called class E addresses and are reserved for experimental use.

IP addresses must be assigned according to the nature of the network during IP address planning in the process of network construction. If the network needs to be connected to the Internet, users need to apply to relevant organizations for IP addresses. IP addresses can be applied from China Internet Network Information Center (CNNIC) in China, and the Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the final IP address assignment. If the network is built to be an internal private network, users do not need to apply for IP addresses and can be assigned dedicated private network addresses.

Table 1-1 Reserved and Available Addresses

Class	Address Range	Status
Class A network	0.0.0.0~0.255.255.255	Reserved
	1.0.0.0~126.255.255.255	Available
	127.0.0.0~127.255.255.255	Reserved
Class B network	128.0.0.0~191.254.255.255	Available
	191.255.0.0~191.255.255.255	Reserved

Class	Address Range	Status
Class C network	192.0.0.0~192.0.0.255	Reserved
	192.0.1.0~223.255.254.255	Available
	223.255.255.0~223.255.255.255	Reserved
Class D network	224.0.0.0~239.255.255.255	Multicast addresses
Class E network	240.0.0.0~255.255.255.254	Reserved
	255.255.255.255	Broadcast addresses

2. Private Network IP Addresses

Private network IP addresses are not used in the Internet. If the devices to which private addresses are assigned need to be connected to the Internet, these IP addresses need to be converted into valid Internet addresses. Table 1-2 lists private network address ranges. Private network addresses are defined in RFC1918 and include three address blocks.

Table 1-2 Private Network Addresses

Class	Address Range	Status
Class A network	10.0.0.0–10.255.255.255	One class A network
Class B network	172.16.0.0–172.31.255.255	16 class B networks
Class C network	192.168.0.0–192.168.255.255	256 class C networks

For assignment of IP addresses, TCP/User Datagram Protocol (UDP) ports, and other codes, refer to RFC1166.

3. Special IP Addresses

The IP addresses listed below are used for special purposes and cannot be used as host IP addresses.

- Addresses with the network ID of all zeros: Indicates the host in the network. For example, 0.0.0.16 indicates the host numbered 16 in the network.
- Addresses with the host ID of all zeros: Indicates a network address, used for identifying a network, for example, 192.168.1.0.
- Addresses with the host ID of all ones: Indicates a broadcast address of the network. For example, the packets with the destination address of 192.168.1.255 will be forwarded to all hosts in the 192.168.1.0 network.

4. Network Mask

A network mask is also a 32-bit value and identifies the bits occupied by the network part of an IP address. In a network mask, the IP address bits corresponding to the bits whose values are ones are the network part, and the IP address bits corresponding to the bits whose values are zeros are the host address. For example, for class A networks, the network mask is 255.0.0.0. Network masks can be used to divide a network into several

subnets. Some bits of the host address are used as the network ID to decrease the host capacity and increase the number of networks. In this case, network masks are called subnet masks.

5. MTU

Maximum transmission unit (MTU) is the maximum size, usually in bytes, of the data transmitted by the data link layer to its upper layer, such as the IP and Multiprotocol Label Switching (MPLS). The MTU is protocol-specific, for example:

- The MTU for IEEE802.3/802.2 is 1,492 bytes.
- The MTU range of an Ethernet port is 64 to 1,518 bytes. Ethernet frames beyond this range may be dropped.

The IP protocol decides whether to fragment data based on the Layer 2 MTU value. Routes between the two devices may go through many hops, and the smallest MTU determines the transmission rate.

6. TTL

Time to live (TTL) refers to the number of network segments, through which packets are allowed to pass before the packets are discarded. The TTL value is used to judge whether packets stay on the network for a long time and should be discarded.

An IP packet is transmitted from the source address to the destination address through routers. A TTL value is set at the source end and decreases by 1 each time the IP packet passes through a router. When the TTL value drops to zero, the router deems the destination unreachable and discards the packet. TTL prevents infinite transmission of useless packets and bandwidth waste.

1.1.3 Principles

1. Obtaining IP Addresses

A device must have an IP address before sending and receiving IP datagrams. Only the interface configured with an IP address can run the IP protocol.

An interface can obtain IP addresses in the following four ways. These ways are mutually exclusive. If you configure a new way to obtain an IP address, the old IP address will be overwritten.

(1) Manually configuring IP addresses

(2) Obtaining IP addresses through the Dynamic Host Configuration Protocol (DHCP): For details about the DHCP protocol, see "Configuring DHCP" in the *IP Configuration Guide*.

(3) Obtaining IP addresses through the Point-to-Point Protocol (PPP) negotiation: A point-to-point interface accepts the IP address assigned by the peer through PPP negotiation. During PPP negotiation, the server checks authentication information of the client. If the client passes the authentication, the server assigns an IP address to the client (if the client is configured with an IP address and the IP address meets requirements of the server, the server approves the IP address of the client). The IP address of the peer can be directly specified or assigned from the address pool.

(4) Borrowing IP addresses of other interfaces: An interface can borrow an IP address from another interface on the same device that is assigned an IP address.

Note

- IP addresses of Ethernet interfaces, tunnel interfaces, and loopback interfaces can be borrowed. However, these interfaces cannot borrow IP addresses from other interfaces.

- The IP addresses of the borrowed interfaces cannot be borrowed from other interfaces.
- If a borrowed interface has multiple IP addresses, only the primary IP address can be borrowed.
- The IP address of one interface can be lent to multiple interfaces.
- IP addresses of borrowing interfaces are always consistent with and change with IP addresses of borrowed interfaces.

2. Configuring Multiple IP Addresses for an Interface

An interface on a device can be configured with multiple IP addresses, of which one is the primary IP address and the others are secondary IP addresses. Theoretically, the number of secondary IP addresses is not limited. However, secondary IP addresses must belong to different networks and secondary IP addresses must be in different networks from primary IP addresses. In network construction, secondary IP addresses are often used in the following circumstances:

- A network does not have enough host addresses. For example, when the number of hosts exceeds 254 in a local area network(LAN), one class C network is not enough and another class C network is needed. In this case, two networks need to be connected. Therefore, more IP addresses are needed.
- Many old networks are based on Layer 2 bridged networks without subnetting. You can use secondary IP addresses to upgrade the network to a routing network based on IP layer. For each subnet, one device is configured with one IP address.
- When two subnets of one network are isolated by another network, in consideration that one subnet cannot be configured on two or more interfaces of a device, you can connect the isolated subnets by creating a subnet on the isolated network and configuring a secondary address.

3. Broadcast Packet Processing

Broadcast packets refer to the packets destined for all hosts on a physical network. The device supports two types of broadcast packets. One type is limited broadcast packets, with the 32-bit destination address of all ones, that is, 255.255.255.255. The other type is directed broadcast packets, with the destination address of all hosts in a specified network, that is, host ID bits of all ones, for example, 192.168.1.255/24. Limited broadcast packets are blocked by the router, whereas directed broadcast packets can be forwarded.

If IP network devices forward limited broadcast packets, the network may be overloaded, which severely affects network performance. This circumstance is called a broadcast storm. Devices provide some approaches to confine broadcast storms within the local network and prevent continuous spread of broadcast storms. Layer 2 network devices such as bridges and switches still forward and spread broadcast storms.

The best way to avoid broadcast storms is to assign a broadcast address to each network, which is directed broadcast. This requires the IP protocol to use directed broadcast packets rather than limited broadcast packets to spread data. When receiving IP directed broadcast packets, the devices that is not directly connected to the destination subnet will forward them in the same way as that for unicast packets. After directed broadcast packets reach the device that is directly connected to the destination subnet, the device converts the directed broadcast mode into limited broadcast mode and broadcasts the packets to all hosts on the destination subnet at the link layer.

For details about broadcast, see RFC919 and RFC922.

4. ICMP Packet

Internet Control Message Protocol (ICMP) is a sub protocol of the TCP/IP protocol suite and is used to transfer control messages between IP hosts and network devices to notify certain devices of packet transmission exceptions. The following describes common ICMP packets.

- Echo request and echo reply

  Common ping operations use echo requests and echo replies. A device sends an echo request to another node. If there is no exception on the way, the destination host returns an echo reply, indicating that the host is reachable.

- Protocol unreachable message

  When a device receives a non-broadcast packet destined for itself and the packet uses the IP protocol that cannot be processed by the device, the device sends an ICMP protocol unreachable message to the source host.

- Host unreachable message

  When a device receives a non-broadcast packet destined for itself but the device does not know a route to forward the packet, it sends an ICMP host unreachable message to the source address.

- Redirection message

  Sometimes a network device sends packets from the interface that receives the packets, indicating that a route may be less than optimal. If this condition occurs, the device will send an ICMP redirection message to the data source, informing the source that the gateway reachable to the destination address is another device on the same subnet. In this way, the data source sends subsequent packets according to the optimal path.

- Mask reply message

  Sometimes, a network device sends an ICMP mask request message to obtain the mask of a subnet. The network device that receives the ICMP mask request message sends a mask reply message.

- TTL timeout error message

  When a device forwards an IP packet, if the TTL expires, the device responds to the source end with a TTL timeout error message.

  To prevent attacks from other devices after the device is located through traceroute, you can disable the function of sending TTL timeout errors on the device. After this function is disabled, the device will no longer make a response when receiving a TTL timeout message.

- Timestamp query

  RFC792 requires the system to return its current time after receiving an ICMP timestamp query request.

  To prevent attackers from obtaining the system time through this protocol and attacking some time-based protocols, you can disable the timestamp query function. Then, the device directly discards received ICMP timestamp query requests.

5. Limiting Transmission Rate of ICMP Error Packets

This function limits the transmission rate of ICMP error packets by using the token bucket algorithm to prevent denial of service (DoS) attacks.

If an IP packet needs to be fragmented but the Don’t Fragment (DF) bit in the header is set to 1, the device returns an ICMP destination unreachable message to the source host. This ICMP error message is used to

discover the path MTU. When there are too many other ICMP error messages, the ICMP destination unreachable message may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable messages and other ICMP error messages respectively.

6. IP MTU

The IP protocol at the network layer checks the size of each packet from the upper layer protocol and determines whether it should be "fragmented" based on the MTU size of the local device.

If an IP packet exceeds the IP MTU size, the device fragments the packet. For all devices on the same physical network segment, the IP MTU of interconnected interfaces must be the same. After the link MTU of interfaces is changed, the IP MTU of interfaces will be changed accordingly. The IP MTU of interfaces automatically keeps consistent with the link MTU of interfaces. However, if the IP MTU of interfaces is adjusted, the link MTU of interfaces will not be changed.

7. IP Source Routing

When a device receives an IP packet, it checks the options such as the strict source route, loose source route, and record route in the IP packet header. These options are detailed in RFC791. If the device detects that the packet enables one option, it performs an action accordingly. If the device detects an invalid option, it returns an ICMP parameter error message to the source and then discards the packet.

After the function of processing IP source routing information is enabled on a device, the source route option is added to an IP packet to test the throughput of a specific network or help the packet bypass the failed network. However, this may cause network attacks such as source address spoofing and IP spoofing.

1.1.4 Protocols and Standards

- RFC1918: Address Allocation for Private Internet
- RFC1166: Internet Numbers
- RFC919: Broadcasting Internet Datagrams
- RFC922: Broadcasting Internet Datagrams Subnets
- RFC791: Internet Protocol
- RFC792: Internet Control Message Protocol

1.2 Configuration Task Summary

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring an IP Address for an Interface
- Configuring the Default Gateway for a Management Interface
- Configuring Directed Broadcast Packets
- Configuring ICMP Messages
- Configuring the Transmission Rate of ICMP Error Messages
- Setting the IP MTU Value
- Setting the IP TTL Value
- Configuring IP Routed Port Protection

- Configuring the IP Source Route Option

1.3 Configuring an IP Address for an Interface

1.3.1 Overview

This section describes how to configure an IP address for an interface for communication over the IP network. IP addresses can be manually configured or obtained through DHCP. In general, an interface only needs to be configured with one IP address to achieve communication with other hosts.

1.3.2 Configuration Tasks

(1) Configure an IP address for an interface. The configuration steps below are mutually exclusive. Please configure only one task.

- Configuring a Static IP Address for an Interface
- Configuring an Unnumbered Interface to Borrow an IP Address
- Configuring an IP Address Combination for an Interface

(2) (Optional) Configuring an IP Broadcast Address

1.3.3 Configuring a Static IP Address for an Interface

1. Restrictions and Guidelines

Manual configuration of IP addresses and dynamic acquisition of IP addresses are mutually exclusive. If you configure a new approach to obtain an IP address, the old IP address will be overwritten.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an IP address for an interface.

ip address *ip-address mask* [**secondary**]

No IP address is configured for an interface by default.

1.3.4 Configuring an Unnumbered Interface to Borrow an IP Address

1. Restrictions and Guidelines

- An Ethernet interface cannot be configured as an unnumbered interface. When the Serial Line Internet Protocol (SLIP), High-Level Data Link Control (HDLC), PPP, Link Access Procedure, Balanced (LAPB), or frame relay is configured on a serial interface, the serial interface can be configured as an unnumbered interface. When frame relay is configured, only a point-to-point subinterface can be configured as an unnumbered interface. An X.25 interface cannot be configured as an unnumbered interface.
- The ping operation cannot be used to check whether an unnumbered interface is working properly because

an unnumbered interface has no IP address.

- You can monitor the status of an unnumbered interface remotely through the Simple Network Management Protocol (SNMP).
- Network startup cannot be carried out through an unnumbered interface.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an unnumbered interface to borrow an IP address.

ip unnumbered *interface-type interface-number*

An unnumbered interface is not configured to borrow an IP address by default.

1.3.5 Configuring an IP Address Combination for an Interface

1. Restrictions and Guidelines

The IP address combination configuration command can be configured only on switch virtual interfaces (SVIs) and management (MGMT) interfaces.

The IP address combination configuration command and the static IP address configuration command as well as DHCP are mutually exclusive, but the IP address combination configuration command can be used to configure both static IP addresses and DHCP.

- When the IP address combination configuration command is used to configure a static IP address, if an IP address on the same network segment is already configured, the configuration fails.
- When the IP address combination configuration command is used to configure both a static IP address and a dynamic IP address, if the IP address obtained through DHCP does not conflict with the network segment of the static IP address, the IP address obtained through DHCP is the primary IP address and the static IP address is a secondary IP address. If the IP address obtained through DHCP conflicts with the network segment of the static IP address, an IP address will be obtained again, during which the static IP address is a primary IP address.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an IP address combination for the interface.

ip address mix { **dhcp** | *ip-address network-mask* }

No IP address combination is configured for an interface by default.

1.3.6 Configuring an IP Broadcast Address

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an IP broadcast address.

ip broadcast-address *ip-address*

The default IP broadcast address of an interface is 255.255.255.255.

1.4 Configuring the Default Gateway for a Management Interface

1.4.1 Overview

This section describes how to configure the default gateway for a management interface. After configuration, a default route is generated, with the outbound interface of the management interface and the next hop of the configured gateway.

1.4.2 Restrictions and Guidelines

This command can be configured on a management interface only.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface mgmt *interface-number*

(4) Configure the default gateway for the management interface.

gateway *ip-address*

No default gateway is configured for a management interface by default.

1.5 Configuring Directed Broadcast Packets

1.5.1 Overview

You can configure a specified interface to forward directed broadcast packets. Then, the interface can forward directed broadcast packets destined for the directly connected network.

1.5.2 Restrictions and Guidelines

- This configuration applies to the transmission of directed broadcast packets within the destination subnet and will not affect the forwarding of other directed broadcast packets.
- On an interface, you can define an access control list (ACL) to control the forwarding of certain directed broadcast packets. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the interface to allow forwarding directed broadcast packets.

ip directed-broadcast [*acl-number*]

The function of translating the IP directed broadcast mode to the physical broadcast mode is disabled by default.

1.6 Configuring ICMP Messages

1.6.1 Overview

The ICMP protocol is used to transfer control messages between IP hosts and network devices to notify network exceptions. You can enable the functions of sending TTL timeout messages, ICMP destination unreachable messages, ICMP redirection messages, and ICMP mask reply messages, and timestamp query function.

1.6.2 Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Enabling the Function of Sending TTL Timeout Messages
- Enabling the Timestamp Query
- Enabling the Function of Sending ICMP Destination Unreachable Messages
- Enabling the Function of Sending ICMP Redirection Messages
- Enabling the Function of Sending ICMP Mask Reply Messages

1.6.3 Enabling the Function of Sending TTL Timeout Messages

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of sending TTL timeout messages.

ip ttl-expires enable

The function of sending TTL timeout messages is enabled by default.

1.6.4 Enabling the Timestamp Query

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the timestamp query function.

ip icmp timestamp

The timestamp query function is enabled by default.

1.6.5 Enabling the Function of Sending ICMP Destination Unreachable Messages

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the function of sending ICMP destination unreachable messages.

ip unreachables

The function of sending ICMP destination unreachable messages is enabled by default.

1.6.6 Enabling the Function of Sending ICMP Redirection Messages

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the function of sending ICMP redirection messages.

ip redirects

The function of sending ICMP redirection messages is enabled by default.

1.6.7 Enabling the Function of Sending ICMP Mask Reply Messages

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the function of sending ICMP mask reply messages.

ip mask-reply

The function of sending ICMP mask reply messages is enabled by default.

1.7 Configuring the Transmission Rate of ICMP Error Messages

1.7.1 Overview

This function limits the transmission rate of ICMP error packets by using the token bucket algorithm to prevent denial of service (DoS) attacks.

If an IP packet needs to be fragmented but the Don't Fragment (DF) bit in the header is set to 1, the device sends an ICMP destination unreachable message to the source host. This ICMP error message is used to discover the path MTU. If there are too many other ICMP error messages, the ICMP destination unreachable packet may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable messages and other ICMP error messages respectively.

1.7.2 Restrictions and Guidelines

Since the precision of the timer is 10 milliseconds, you are advised to set the refresh cycle of a token bucket to an integer multiple of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the transmission rate is set to 1 packet per 5 milliseconds, two ICMP error packets are actually sent per 10 milliseconds. If the refresh cycle is not an integral multiple of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted into an integral multiple of 10 milliseconds. For example, if the transmission rate is set to 3 packets per 15 milliseconds, two ICMP error packets are actually sent per 10 milliseconds.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the transmission rate of ICMP error packets.

ip icmp error-interval [**df**] *interval* [*bucket-size*]

Ten ICMP error packets are transmitted within 100 milliseconds by default.

1.8 Setting the IP MTU Value

1.8.1 Overview

This section describes how to set the MTU of an IP packet. If the size of an IP packet exceeds the IP MTU size, the packet will be fragmented.

1.8.2 Restrictions and Guidelines

For all devices on the same physical network segment, the IP MTU of interconnected interfaces must be the same. The IP MTU of interfaces automatically keeps consistent with the link MTU of interfaces. If the link MTU of interfaces is changed, the IP MTU of interfaces will be changed accordingly. However, if the IP MTU of interfaces is adjusted, the link MTU of interfaces will not be changed.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Set the IP MTU.

ip mtu *mtu*

The default MTU of an IP packet is 1500 bytes.

1.9 Setting the IP TTL Value

1.9.1 Overview

When an IP packet is transmitted from the source address to the destination address through routers, a TTL value is set at the source end and decreases by 1 every time that the IP packet passes through a router. When the TTL value drops to zero, the router discards the packet. TTL prevents infinite transmission of useless packets and waste of bandwidth.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the IP TTL.

ip ttl

The default TTL value of unicast packets sent by the device is 64.

1.10 Configuring IP Routed Port Protection

1.10.1 Overview

This section describes how to enable routed port protection to prevent packets from being transmitted through the same interface that receives the packets.

1.10.2 Restrictions and Guidelines

This command can only be used for Layer 3 routed ports.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the IP routed port protection.

ip redirect-drop

The IP routed port protection function is disabled by default.

1.11 Configuring the IP Source Route Option

1.11.1 Overview

The IP source route option is used to test the throughput of a specific network and help the packet bypass a failed network.

1.11.2 Restrictions and Guidelines

Enabling the IP source route option may cause network attacks such as source address spoofing and IP spoofing.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IP source route option.

ip source-route

The IP source route option is enabled by default.

1.12 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

Table 1-3 Monitoring

Command	Purpose
show ip interface [*interface-type interface-number* | **brief**]	Displays the IP address of an interface.
show ip packet statistics [**total** | *interface-type interface-number*]	Displays IP packet statistics.
show ip packet queue	Displays the statistics on sent and received IP packets in the protocol stack.
show ip raw-socket [*protocol-number*]	Displays all IPv4 raw sockets.
show ip sockets	Displays all IPv4 sockets.
show ip udp [**local-port** *port-number* | **peer-port** *port-number*]	Displays all IPv4 UDP sockets.
show ip udp statistics	Displays the statistics on all IPv4 UDP sockets.

1.13 Configuration Examples

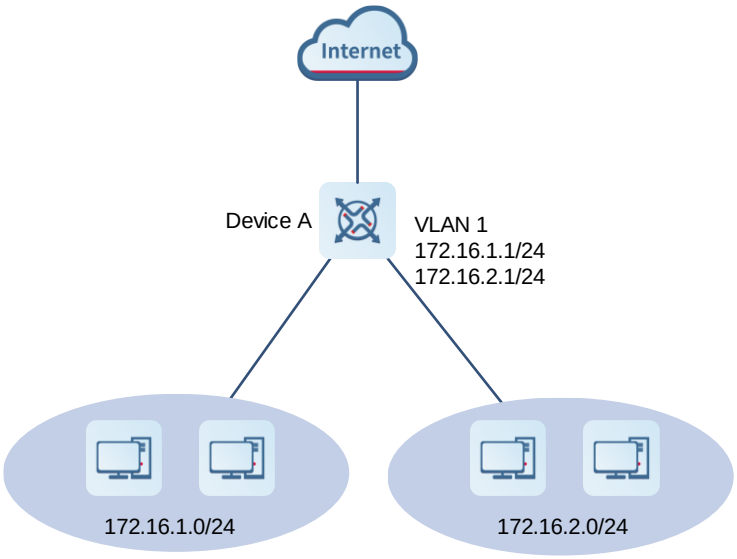
1.13.1 Configuring IPv4 Addresses for Network Communication

1. Requirements

As shown in Figure 1-5, device A is connected to a LAN (belonging to VLAN 1), which involves two network segments: 172.16.1.0/24 and 172.16.2.0/24. Computers on the two network segments are required to access the Internet through device A and hosts on the two network segments can also communicate with each other.

2. Topology

Figure 1-5 Topology of Configuring IPv4 Addresses for Network Communication



3. Notes

- Configure two IP addresses on the interface VLAN 1, of which one is a primary IP address and the other is a slave IP address.
- Configure the device as the gateway on the hosts on these two network segments.

4. Procedure

(1) Configure device A.

Configure a primary IP address and a slave IP address for the interface VLAN 1.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface vlan 1
DeviceA(config-if-VLAN 1)# ip address 172.16.1.1 255.255.255.0
DeviceA(config-if-VLAN 1)# ip address 172.16.2.1 255.255.255.0 secondary
```

(2) Configure the hosts on the 172.16.1.0/24 network segment.

Set the gateway to 172.16.1.1/24 for the hosts.

(3) Configure the hosts on the 172.16.2.0/24 network segment.

Set the gateway to 172.16.2.1/24 on the hosts.

5. Verification

Run the **ping** command on device A to check the connectivity with the hosts in the 172.16.1.0/24 network segment.

```
DeviceA# ping 172.16.1.2
Sending 5, 100-byte ICMP Echoes to 172.16.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **ping** command on device A to check the connectivity with the hosts in the 172.16.2.0/24 network segment.

```
DeviceA# ping 172.16.2.1
Sending 5, 100-byte ICMP Echoes to 172.16.2.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **ping** command to check the connectivity between the hosts in the 172.16.1.0/24 network segment and the hosts in the 172.16.2.0/24 network segments.

6. Configuration Files

Device A

```
hostname DeviceA
!
interface vlan 1
 ip address 172.16.1.1 255.255.255.0
 ip address 172.16.2.1 255.255.255.0 secondary
!
```

Contents

1 Configuring DHCP 1
1.1 Introduction 1
1.2 Principles 2
1.2.1 Basic Concepts 2
1.2.2 Message Format 3
1.2.3 DHCP Lease Process 6
1.2.4 DHCP Server 7
1.2.5 DHCP Relay Agent 8
1.2.6 DHCP Associated with VRRP Monitoring 12
1.2.7 Protocols and Standards 13
1.3 Configuring DHCP Server 13
1.3.1 Overview 13
1.3.2 Configuration Task Summary 13
1.3.3 Enabling DHCP Server 13
1.3.4 Configuring Static IP Address Assignment 14
1.3.5 Configuring Dynamic Assignment of IP Addresses and Network Parameters 15
1.3.6 Configuring DHCP Address Pool Management Function 16
1.3.7 Providing the Boot Image File Name 18
1.3.8 Assigning IP Addresses Based on Class Rules 18
1.3.9 Assigning IP Addresses Based on AM Rules 20
1.3.10 Refreshing Trusted ARP Entries 20
1.3.11 Configuring Rogue DHCP Server Detection 21

1.3.12 Configuring IP Address Conflict Detection....21

1.3.13 Configuring Compulsory NAK Reply....23

1.3.14 Configuring VRRP Monitoring....23

1.3.15 Configuring ARP-based Go-Offline Detection....24

1.3.16 Saving Historical Leases....24

1.4 Configuring DHCP Relay....25

1.4.1 Overview....25

1.4.2 Configuration Task Summary....25

1.4.3 Configuring Basic DHCP Relay Functions....25

1.4.4 Configuring Option 82....26

1.4.5 Configuring Server-ID Check....26

1.4.6 Enabling DHCP Relay Suppression....27

1.4.7 Configuring Multiple Gateway IP Addresses....27

1.4.8 Forcing a DHCP Relay to Send a Reply Packet....28

1.4.9 Configuring the Source IP Address of DHCP Relay Packets....28

1.5 Monitoring....29

1.6 Configuration Examples....30

1.6.1 Configuring Static Address Binding....30

1.6.2 Dynamically Assigning IP Addresses....31

1.6.3 Configuring DHCP Relay....34

1.6.4 Assigning IP Addresses Based on Class Rules....36

1 Configuring DHCP

1.1 Introduction

1. Overview

Dynamic Host Configuration Protocol (DHCP) is a local area network (LAN) protocol that dynamically assigns reusable network addresses and additional configurations to hosts. DHCP uses User Datagram Protocol (UDP) as its transport protocol to send and receive DHCP messages through port 67.

DHCP works in client/server mode. A DHCP client sends a request message to a DHCP server for an IP address and other configurations. When a DHCP client and a DHCP server are not in the same subnet, they need a DHCP relay agent to forward DHCP request and reply messages.

2. Origin and Development

DHCP originates from the Bootstrap Protocol (BOOTP), which is used by diskless hosts to obtain their own IP addresses, server IP address, boot image file name, gateway IP address, and other information from a server. BOOTP is designed for static environments. It requires the hardware address of a host be manually added to the BOOTP table and mappings between hardware addresses and IP addresses be static. In other words, BOOTP is less dynamic. In an environment with limited IP addresses, one-to-one mapping of BOOTP wastes IP addresses.

As the network scale expands and network complexity increases, BOOTP designed for static hosts can no longer meet requirements in wireless network scenarios and scenarios in which the number of computers exceeds the number of available IP addresses.

Therefore, the Internet Engineering Task Force (IETF) proposes a new protocol, that is, DHCP. DHCP is an enhanced version of BOOTP and consists of a server and a client. A DHCP server centrally manages all IP network settings and processes DHCP requests from DHCP clients. DHCP clients use the IP environment data assigned by the DHCP server. Compared with BOOTP, DHCP employs the lease concept to allocate clients' TCP/IP settings effectively and dynamically. DHCP also meets compatibility requirements of BOOTP clients.

3. Benefits

During network construction, a DHCP server can bring the following benefits:

- Low network access cost: Generally, the network access cost in static address assignment mode is higher than that in dynamic address assignment mode.
- Simplified configuration and low network construction cost: Dynamic address assignment significantly simplifies device configuration and reduces the deployment cost if no professional technical personnel are available to deploy devices.
- Centralized management: You can modify configurations for multiple subnets by simply modifying the DHCP server configuration.

1.2 Principles

1.2.1 Basic Concepts

- DHCP server

  A DHCP server is implemented based on RFC 2131. It assigns IP addresses to hosts and manages these IP addresses.

- DHCP client

  A DHCP client enables a device to automatically obtain an IP address and other configurations from a DHCP server.

- DHCP relay

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

- Lease time

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

- Address pool

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

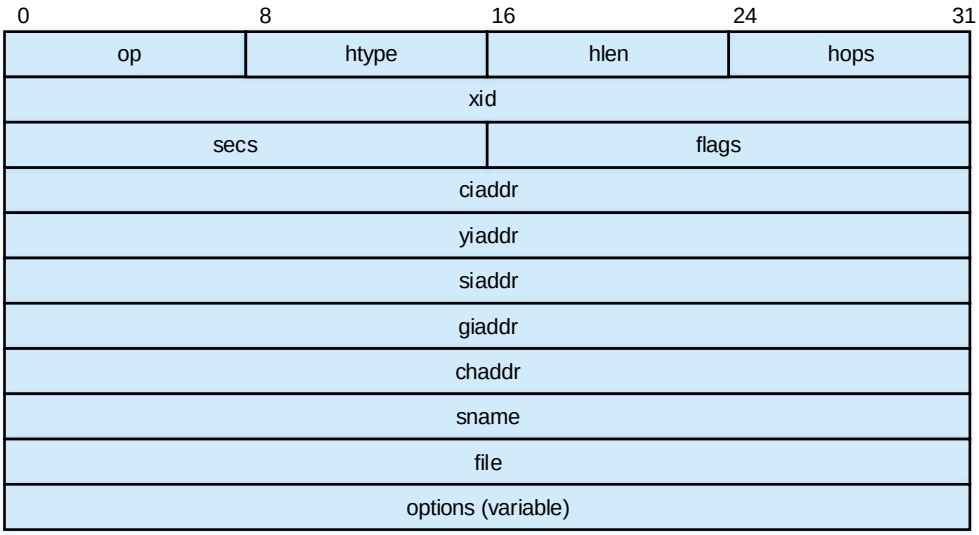
- Option type

  An option type is a parameter specified by a DHCP server when it provides the lease service to a DHCP client. For example, common options include the IP addresses of the default gateway (router), Windows Internet Name Service (WINS) server, and Domain Name System (DNS) server. A DHCP server also allows configuration of other options. Most options are predefined in RFC 2132. You can add user-defined options.

1.2.2 Message Format

1. DHCP Packet

Figure 1-1 DHCP Packet



The following describes fields contained in a DHCP packet:

- **op**: Packet type, including request packets and reply packets. A packet with **op** set to **1** is a request, and a packet with **op** set to **2** is a reply. The specific packet type is identified by the **options** field.
- **htype** (hardware type): Hardware address type of a DHCP client. For Ethernet clients, the field value is **1**.
- **hlen** (hardware length): Length of the hardware address of a DHCP client. For Ethernet clients, the field value is **6**.
- **hops**: Number of DHCP relay agents that a DHCP packet passes through. The field value increments by 1 each time a DHCP request packet passes through one DHCP relay agent.
- **xid**: Random number selected by a DHCP client when it sends a request. It is used to identify an address requesting process.
- **secs**: Time (in seconds) elapsed since a DHCP client starts a DHCP request.
- **flags**: The first bit is the broadcast reply flag bit and is used to identify whether a DHCP server sends a reply packet in unicast or broadcast mode. **0** indicates unicast, and **1** indicates broadcast. The other 15 bits are set to **0**.
- **ciaddr** (client IP address): IP address of a DHCP client. If a client has a valid and available IP address, add it to this field. During initialization, the client does not have an IP address, and this field is set to **0.0.0.0**. This field is not used to apply for a specific IP address by the client.
- **yiaddr** (your client IP address): IP address assigned by a DHCP server to a DHCP client.
- **siaddr** (server IP address): IP address of the server from which a DHCP client obtains boot configurations.
- **giaddr** (gateway IP address): IP address of the first DHCP relay agent that a request packet of a DHCP client passes through.
- **chaddr** (client hardware address): Hardware address of a DHCP client.

- **sname** (server name): Name of the server from which a DHCP client obtains boot configurations.
- **file**: Boot configuration file name and path specified by a DHCP server for a DHCP client.
- **options**: Optional fields with variable length, including the packet type, valid lease time, IP address of the DNS server, and IP address of the WINS server.

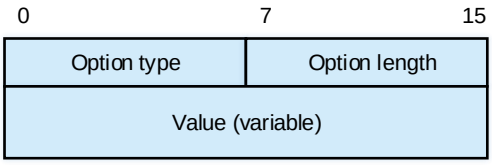
2. Message Types

- DHCP DISCOVER: first message broadcast by a DHCP client for DHCP interaction when it accesses a network for the first time.
- DHCP OFFER: message sent by a DHCP server in response to the DHCP DISCOVER message. The message carries various configuration parameters.
- DHCP REQUEST: This message has the following functions:
  - After a client is initialized, it broadcasts a DHCP REQUEST message to respond to the DHCP OFFER message of a DHCP server.
  - After a client is restarted and initialized, it broadcasts a DHCP REQUEST message to confirm the previously assigned IP address and other configurations.
  - After a client is bound to an IP address, it sends a DHCP REQUEST message to update the IP address lease.
- DHCP ACK: acknowledgment message of a server in response to a client's DHCP REQUEST message. A client obtains an IP address and related configuration parameters only after receiving this message.

3. Option Format

A DHCP server uses the **Options** field to transfer control information and network configuration parameters to dynamically assign IP addresses and provide rich network configurations to clients. The **Options** field consist of the type, length, and value parts. Figure 1-2 shows the format.

Figure 1-2 Option Format



- **Option type**: option number.
- **Option length**: length of the information content.
- **Value**: information content.

4. Common DHCP Options

The type value of the **Options** field ranges from 1 to 255. Common DHCP options include:

- Option 1: subnet mask.
- Option 3: gateway address.
- Option 6: DNS address.
- Option 15: domain name.
- Option 33: static route. This option contains a group of classified static routes (that is, the mask of the

destination network address is a natural mask and cannot be used for subnet division). After a client receives this option, it adds these static routes to the routing table. If Option 33 and Option 121 coexist, Option 33 is ignored.

- Option 51: IP address lease time.
- Option 53: DHCP message type.
- Option 55: parameter request list. A client uses this option to specify the network configurations that need to be obtained from a server. The option content is the values of parameters requested by a client.
- Option 121: classless static route. This option contains a group of classless static routes (that is, the mask of the destination network address is any value and subnets can be divided by mask). After a client receives this option, it adds these static routes to the routing table. If Option 33 and Option 121 coexist, Option 33 is ignored.

For details about more DHCP options, see RFC 2132 and RFC 3442.

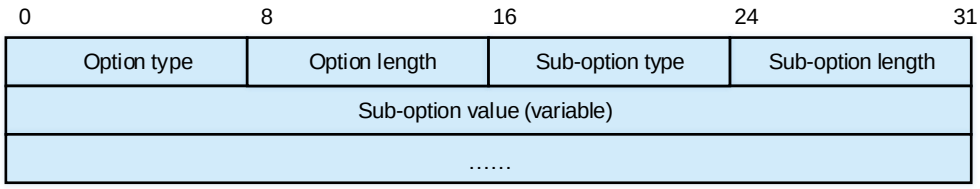
5. User-Defined DHCP Options

- Option 43: specific vendor information

  A DHCP server uses Option 43 to assign specific vendor information to a client. Option 43 uses several sub-options to assign different network configurations to users. The sub-option fields are as follows:

  - **Sub-option type**: type of a sub-option. The value can be **0x01** (ACS parameter), **0x02** (service provider identifier), or **0x80** (PXE boot server address).
  - **Sub-option length**: length of a sub-option.
  - **Sub-option value**: value of a sub-option.

Figure 1-3 Option 43

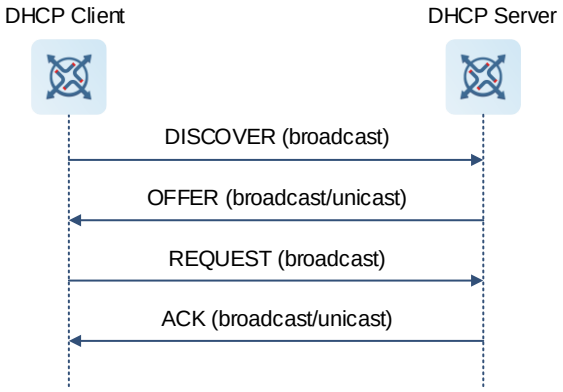


- Option 82: relay agent information

  Option 82 records the location information of a DHCP client. When a DHCP relay agent receives a request packet destined for a DHCP server from a DHCP client, the DHCP relay agent adds Option 82 to the packet and forwards the packet to the DHCP server. An administrator obtains the DHCP client location information from Option 82 to locate the DHCP client, assign an address in a specific range to the client, and control the client security and accounting.

1.2.3 DHCP Lease Process

Figure 1-4 DHCP Lease Process



A DHCP client requests an IP address as follows:

(1) The DHCP client broadcasts a DHCP DISCOVER packet to find a DHCP server in the network.

(2) The DHCP server sends a DHCP OFFER packet to the client in unicast/broadcast mode based on the broadcast bit in the **flags** field of the DISCOVER packet, with the packet containing an IP address, a Media Access Control (MAC) address, a domain name, and a lease time.

(3) The DHCP client broadcasts a DHCP REQUEST packet to formally request an IP address from the DHCP server.

(4) The DHCP server searches for the corresponding lease record based on the MAC address carried in the DHCP REQUEST packet.

- If the lease record exists, the DHCP server sends a DHCP ACK packet to the DHCP client. After receiving the DHCP ACK packet, the DHCP client sends a free Address Resolution Protocol (ARP) packet to check whether another host uses the IP address assigned by the DHCP server. If the DHCP client does not receive a response within the specified time, the DHCP client uses the assigned IP address. If the DHCP client finds IP address conflict, it sends a DHCP DECLINE message to notify the server and requests another IP address from the server after 10s.
- If the lease record does not exist or the DHCP server cannot assign an IP address to the client due to some reasons, the DHCP server sends a DHCP NAK packet to inform the DHCP client that no proper IP address can be assigned. The DHCP client needs to send another DHCP DISCOVER packet to apply for a new IP address.

Note

- The DHCP client may receive DHCP OFFER packets from multiple DHCP servers, but usually it accepts only the first DHCP OFFER packet.
- In addition, the address specified in the DHCP OFFER packet is not necessarily assigned to the client. Generally, the DHCP server reserves this address until the client sends a DHCP REQUEST packet.
- A client broadcasts a DHCP REQUEST packet to inform all DHCP servers that respond with DHCP OFFER packets. The servers not selected by the DHCP REQUEST message will release the previously assigned IP address.

1.2.4 DHCP Server

1. Address Pool

After a DHCP server receives a client's request, it chooses a valid address pool, determines an available IP address from the pool by using the ping mechanism, and delivers the pool configurations and IP address to the client. In addition, the server saves the lease information locally for validity check upon lease renewal.

Address pool configurations include the IP address range, gateway address, DNS address, and lease time.

2. Address Management Method and Assignment Policy

A DHCP server selects an IP address for a client based on the following sequence:

(1) The DHCP server selects an IP address statically bound to the MAC address of the client from its own database.

(2) The DHCP server selects an IP address previously used by the client, that is, the address specified in the IP address option of the DHCP DISCOVER packet sent by the client.

(3) The DHCP server selects an available IP address first found from the DHCP address pool.

(4) If no available IP address is found from the DHCP address pool, the DHCP server checks whether an expired or conflicted IP address exists. If yes, it assigns an available IP address to the client. If not, it reports an error.

3. ARP Entry Check

The ARP entry check function can be used together with the ping mechanism to detect IP address conflicts. If a firewall is enabled on hosts in an actual environment, the ping operation for address conflict detection of a DHCP server becomes invalid. DHCP clients that dynamically apply for IP addresses may be assigned with the same IP address. Address conflict may occur. If the ARP entry check function is enabled, the DHCP server queries the ARP entries after detecting an IP address conflict by using the ping operation. If an ARP entry exists for the IP address to be assigned and is inconsistent with the MAC address of the client to which the IP address is assigned, the DHCP server regards that the IP address is occupied by another user.

You are not advised to enable the ARP entry check function in an environment with ARP attacks. Otherwise, the IP address assignment is affected, resulting in slow or failed IP address assignment.

4. Compulsory NAK Reply

In wireless applications, DHCP clients usually move from one network to another. When receiving a REQUEST packet from a client for lease renewal, a DHCP server replies with a NAK packet for the client if the server finds that the network segment of the client is changed or the lease expires. Such practice avoids the DHCP client from repeatedly sending REQUEST packets and avoids the DHCP client from obtaining an IP address only after the REQUEST packet times out.

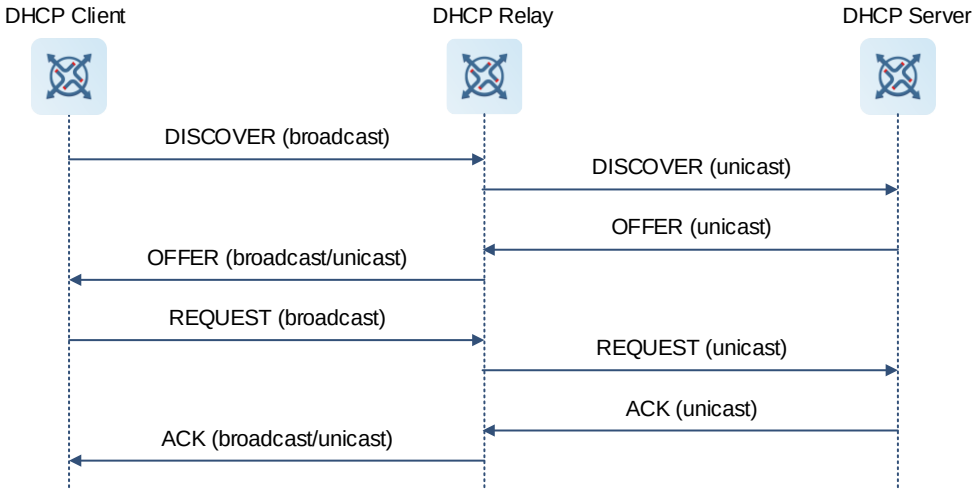
However, the DHCP server can send NAK packets only to its managed DHCP clients because it has lease records of its managed clients only. When a DHCP client moves from another network to the local network, if the DHCP server cannot find the corresponding lease record locally, the DHCP server does not reply with a NAK packet. In this case, the DHCP client needs to send REQUEST packets repeatedly. The client can obtain an IP address again only when the request times out. The time for obtaining an IP address is lengthened. This case also occurs when a client requires lease renewal but the DHCP server loses the lease record of the client due to a restart. In this case, you can configure compulsory NAK reply for the DHCP server if no lease record is found, so as to ensure that the client can obtain an IP address quickly.

1.2.5 DHCP Relay Agent

1. Principles

A DHCP relay agent helps to implement dynamic IP address assignment across network segments. The DHCP relay agent transparently forwards DHCP packets in unicast mode between a DHCP server and DHCP clients that reside on diverse network segments. It serves as a repeater. The Client-Relay-Server mode achieves dynamic management of IP addresses across multiple network segments with only one DHCP server.

Figure 1-5 Working Process

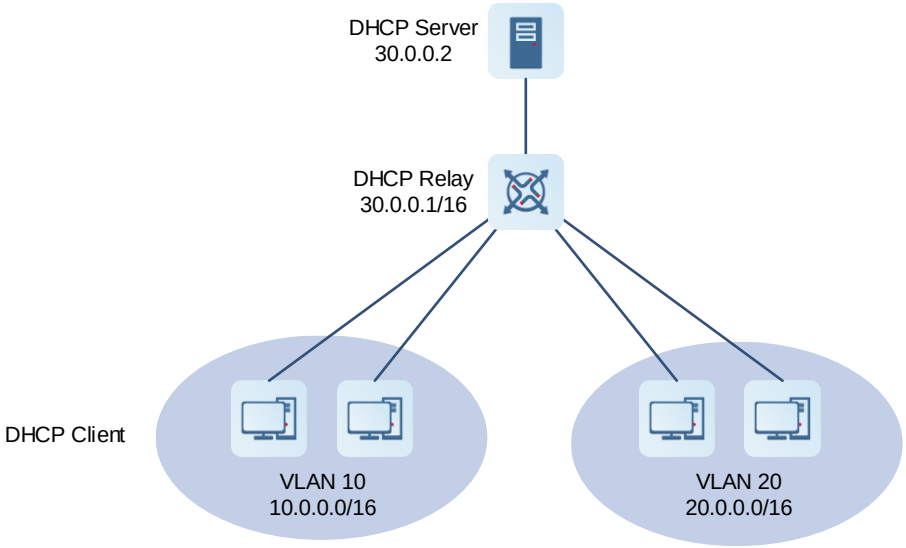


(1) After a DHCP relay agent receives a DHCP DISCOVER or DHCP REQUEST packet broadcast by a DHCP client, the DHCP relay agent adds its own IP address to the **giaddr** field of the packet and forwards the packet to a specified DHCP server in unicast mode.

(2) Based on the **giaddr** field, the DHCP server assigns an IP address and other configurations to the client, so that the DHCP relay agent forwards the configurations to the client, ensuring dynamic client configuration.

2. Typical Applications

Figure 1-6 DHCP Relay Application Scenario



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

3. Option 82

As defined in RFC 3046, a DHCP relay agent can add the DHCP relay agent information option to indicate a DHCP client's network information, so that a DHCP server can assign IP addresses of various privileges based on more accurate information. The option is called Option 82.

Based on the physical port that receives DHCP request packets and the MAC address of the device, the DHCP relay agent constructs Option 82. Option 82 can contain a maximum of 255 sub-options. If Option 82 is defined, it should contain at least one sub-option. Currently, the device supports sub-option 1 (**Circuit ID**) and sub-option 2 (**Remote ID**). Figure 1-7 and Figure 1-8 show the formats of the two sub-options.

Figure 1-7 Option 82 Circuit ID

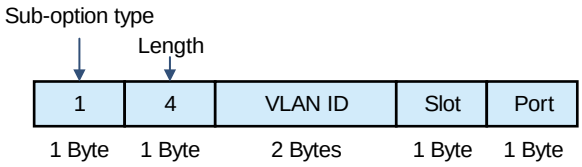
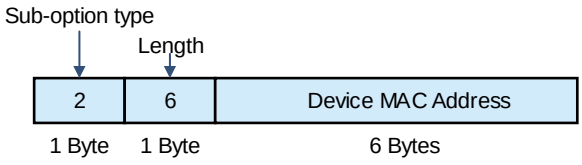


Figure 1-8 Option 82 Remote ID



4. Custom Option 82

Option 82 can be customized. A DHCP relay agent can form an Option 82 based on the physical port that receives DHCP request packets and the MAC address and the name of the device. Figure 1-9 and Figure 1-10 show the formats of the sub-options.

Figure 1-9 Custom Option 82 Circuit ID

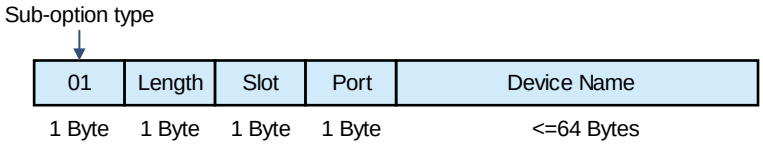
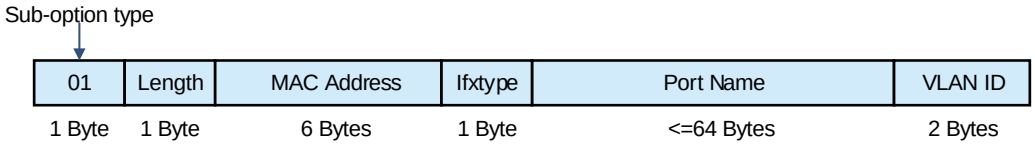


Figure 1-10 Custom Option 82 Remote ID

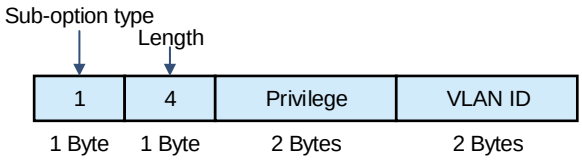


5. Option Dot1x

Option Dot1x should be used in combination with 802.1X authentication and Ruijie's RG-SAM authentication and accounting management system.

A DHCP relay agent constructs the **Circuit ID** sub-option based on the IP privilege delivered during 802.1X authentication and the VLAN ID of a DHCP client. Figure 1-11 shows the option format.

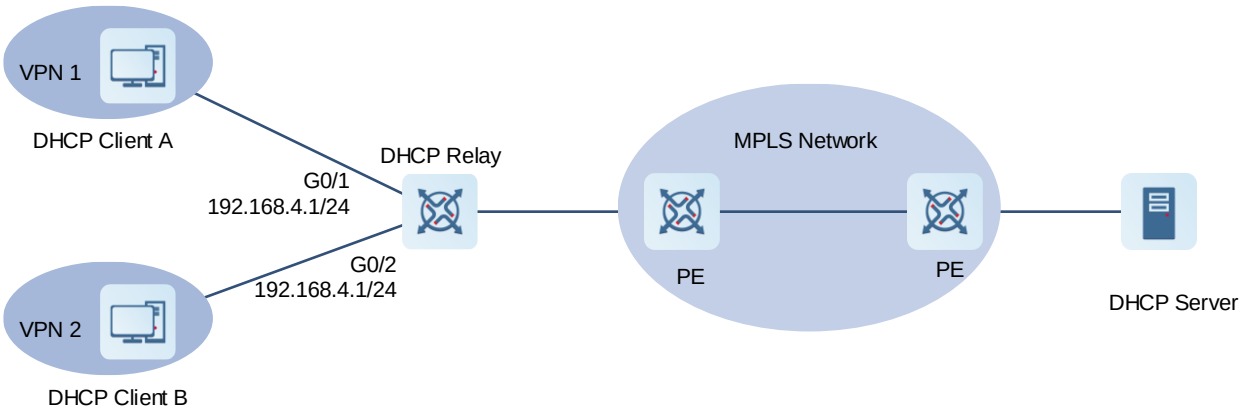
Figure 1-11 Option Dot1x Circuit ID Sub-option



6. Option VPN

Option virtual private network (VPN) should be used in combination with Multiprotocol Label Switching (MPLS) VPN functions.

Figure 1-12 Application in an MPLS VPN Environment



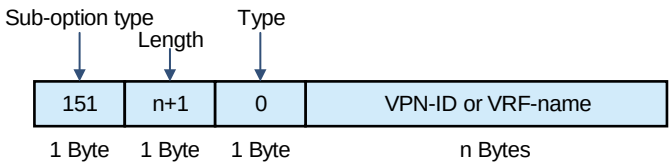
As shown in Figure 1-12, in an MPLS VPN environment, DHCP Client A is connected to GigabitEthernet 0/1 on a DHCP relay agent, and DHCP Client B is connected to GigabitEthernet 0/2 on the DHCP relay. GigabitEthernet 0/1 and GigabitEthernet 0/2 belong to different virtual routing and forwarding (VRF) instances. DHCP Client A and DHCP Client B obtain IP addresses through DHCP. According to the network plan, VPN 1 and VPN 2 share the network segment 192.168.4.0/24. In this case, traditional DHCP application cannot meet the deployment requirement.

To support DHCP Relay in the MPLS VPN environment, Option VPN is introduced, which includes three sub-options, namely, **VPN-ID**, **Subnet-Selection**, and **Server-Identifier-Override**.

- VPN-ID

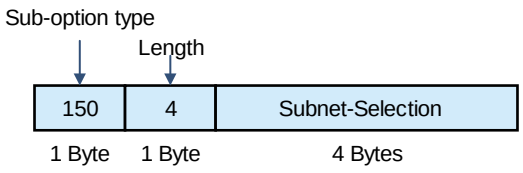
  When a DHCP relay agent receives a DHCP request packet, it adds the VPN information of the DHCP client to the packet as an option. The DHCP server retains **VPN-ID** in a reply packet, so that the DHCP relay agent forwards the packet to the correct VRF instance based on the option. Figure 1-13 shows the option format.

Figure 1-13 VPN-ID



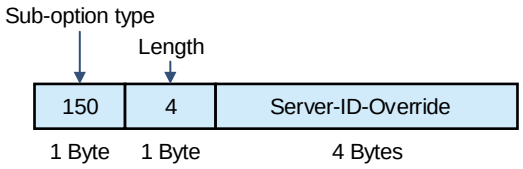
- **Subnet-Selection**: In a traditional DHCP Relay environment, the **giaddr** field is used to indicate information about a client's network and the addresses of a DHCP server and a DHCP relay agent. In an MPLS VPN environment, set **giaddr** to the IP address of an interface on a DHCP relay agent connected to a DHCP server, so that the server can communicate directly with the relay. The client's subnet must be indicated by the **Subnet-Selection** option. Figure 1-14 shows the option format.

Figure 1-14 Subnet-Selection



- **Server-ID-Override**: In an MPLS VPN environment, request packets from a DHCP client cannot be directly sent to a DHCP server. A DHCP relay agent uses this option to carry the IP address of the interface directly connected to the DHCP client. When the server sends a reply packet, this option overrides the **Server-Identifier** option. In this way, the DHCP client sends packets to the DHCP relay agent, and the DHCP relay agent forwards them to the DHCP server. Figure 1-15 shows the option format.

Figure 1-15 Server-Identifier-Override



1.2.6 DHCP Associated with VRRP Monitoring

In a Virtual Router Redundancy Protocol (VRRP) scenario, DHCP provides a command to monitor the VRRP status of the current interface. For interfaces configured with a VRRP address and VRRP monitoring, a DHCP server processes DHCP clients' request packets from an interface on a master device but discards the request packets from an interface on a backup device. If no VRRP address is configured on an interface, the DHCP server does not monitor the VRRP status and processes all DHCP request packets from this interface. VRRP monitoring is configured only on Layer 3 interfaces. It is disabled by default, namely, only the master device provides the DHCP service.

- Assigning IP addresses based on VLANs and ports

  In an environment with an IP address pool, a specified IP address range is assigned for each VLAN and port. A valid address is selected when the normal dynamic address assignment logic is met. There are three scenarios.

  - Global default configuration: Globally configured addresses are assigned by default.
  - Configuration based on VLANs and ports: Addresses in a specified IP address range are assigned only to the clients with specified VLANs and ports.
  - Hybrid configuration: Clients with specified VLANs and ports are assigned with the addresses in the specified IP address range, and the other clients are assigned with default global addresses.

- Preferentially assigning the DNS address obtained from an external DHCP server

  When some ports on the device operate in Point-to-Point Protocol over Ethernet (PPPoE) or DHCP client mode, the device can automatically obtain a DNS address from an external DHCP server and configure the address on the DHCP server of the local device, so that users do not need to perform DNS configuration.

When the device serves as a DHCP server, it preferentially uses the DNS server address obtained from an external DHCP server as the DNS server address in configuration information sent to the DHCP client.

1.2.7 Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 3046: DHCP Relay Agent Information Option
- RFC 3442: Classless Static Route Option for DHCPv4

1.3 Configuring DHCP Server

1.3.1 Overview

Configure the device as a DHCP server to assign IP addresses to DHCP clients and manage these IP addresses and other configurations. You can also configure other custom functions for the DHCP server as required to customize DHCP services.

1.3.2 Configuration Task Summary

(1) Enabling DHCP Server

(2) (Optional) Configuring Static IP Address Assignment

(3) Configuring Dynamic Assignment of IP Addresses and Network Parameters

(4) (Optional) Configuring DHCP Address Pool Management Function

(5) (Optional) Providing the Boot Image File Name

(6) (Optional) Assigning IP Addresses Based on Class Rules

(7) (Optional) Assigning IP Addresses Based on AM Rules

(8) Configuring security functions of a DHCP server: All the configuration tasks below are optional. Perform the configuration tasks as required.

- Refreshing Trusted ARP Entries
- Configuring Rogue DHCP Server Detection

(9) Configuring other custom functions of the DHCP server: All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring IP Address Conflict Detection
- Configuring Compulsory NAK Reply
- Configuring VRRP Monitoring
- Configuring ARP-based Go-Offline Detection
- Saving Historical Leases

1.3.3 Enabling DHCP Server

1. Overview

For the device to function as a DHCP server and assign IP addresses and other network parameters to DHCP clients, enable the DHCP Server function on the device.

2. Restrictions and Guidelines

The **service dhcp** command enables both the DHCP server and DHCP relay functions. When the device is configured with a valid address pool, it acts as a server and directly processes packets. Otherwise, it serves as a relay and forwards the packets.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the DHCP server function.

service dhcp

The DHCP server function is disabled by default.

1.3.4 Configuring Static IP Address Assignment

1. Overview

Deliver specific IP addresses and configurations to specific DHCP clients, such as servers and printers.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Configure the IP address and network mask of a client host.

host *ip-address* [*netmask*]

No IP address or network mask is configured for a client host by default.

If no network mask is defined, the DHCP server uses the natural mask of the IP address as the network mask.

(5) Configure the hardware address or unique ID of a client. Select either of the following configuration tasks.

- Configure a client hardware address.

  hardware-address *hardware-address* [*type*]

  No hardware address is configured by default. If no hardware platform protocol is defined when the hardware address is configured, the default protocol is **ethernet**.

- Configure a unique client ID.

  client-identifier [*unique-identifier*]

  No DHCP client ID is configured by default.

  A client ID consists of the media type, MAC address, and interface name.

(6) (Optional) Configure a client name.

client-name *client-name*

No client name is configured by default. A client name can be any characters in the American Standard Code for Information Interchange (ASCII) character set. The name should not contain the domain name.

1.3.5 Configuring Dynamic Assignment of IP Addresses and Network Parameters

1. Overview

Configure address pool attributes, such as the address lease time, DNS address, and custom options. A DHCP server can use options to send the information to clients, so as to ensure dynamic network parameter assignment.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Configure the primary network segment for dynamic assignment in a DHCP address pool.

network *network-number net-mask* [*low-ip-address high-ip-address*]

No primary network segment for dynamic assignment in a DHCP address pool is configured by default.

(5) (Optional) Configure the default gateway for a client.

default-router { *ip-address*&<1-8> }

No default gateway is configured for a DHCP client by default.

The gateway address that a DHCP server specifies for a DHCP client must be in the same network segment as the address assigned to the client.

(6) (Optional) Configure the domain name for a client.

domain-name *domain-name*

No domain name is configured for a DHCP client by default.

After a DHCP client obtains a specified domain name, it can directly use its host name to access a host whose name contains the same domain name.

(7) (Optional) Configure the DNS server to be assigned to a DHCP client.

dns-server { *ip-address*&<1-8> }

No DNS server is configured for a DHCP client by default.

When multiple DNS servers are defined, the first defined DNS server has the highest priority. A DHCP client selects the next DNS server only when it fails to communicate with the first defined DNS server.

(8) (Optional) Configure the NetBIOS WINS server for a DHCP client.

netbios-name-server { *ip-address*&<1-8> }

No NetBIOS WINS server is configured for a DHCP client by default.

When multiple NetBIOS WINS servers are defined, the first defined NetBIOS WINS server has the highest priority. A DHCP client selects the next NetBIOS WINS server only when it fails to communicate with the first defined NetBIOS WINS server.

(9) (Optional) Configure the type of a NetBIOS node to be assigned to a DHCP client.

netbios-node-type *type*

The default node type of a DHCP client running a Microsoft operating system is broadcast or hybrid. If no WINS server is configured, the client is a broadcast node. Otherwise, it is a hybrid node.

(10) (Optional) Define DHCP server options.

option *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

No DHCP server option is defined by default.

1.3.6 Configuring DHCP Address Pool Management Function

1. Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring an Address Lease Time
- Adding Trusted ARP Entries During Address Assignment
- Forcibly Disabling Gateway Assignment
- Enabling or Disabling an Address Pool
- Configuring an Alarm Threshold for an Address Pool

2. Configuring an Address Lease Time

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Configure an address lease time.

lease { *days* [*hours*] [*minutes*] | **infinite** }

The default lease time of a static address pool is permanent by default. The default lease time of other address pools is 1 day.

3. Adding Trusted ARP Entries During Address Assignment

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Add trusted ARP entries.

update arp

No trusted ARP entry is added during DHCP address assignment by default.

4. Forcibly Disabling Gateway Assignment

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Forcibly disable gateway assignment.

force-no-router

A DHCP server assigns a gateway to a DHCP client by default.

5. Enabling or Disabling an Address Pool

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Enable or disable the address pool.

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

A created address pool is enabled by default.

6. Configuring an Alarm Threshold for an Address Pool

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Configure an alarm threshold for the address pool.

lease-threshold *threshold-percentage*

The default alarm threshold is 90% for the address pool.

1.3.7 Providing the Boot Image File Name

1. Overview

Some DHCP clients need to download the operating system or configuration file in the boot process. A DHCP server must provide the required image file name during boot for a DHCP client to download the file from the corresponding server.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) (Optional) Configure the list of boot servers that a DHCP client needs to access during boot.

next-server { *ip-address*&<1-8> }

No list of boot servers that a DHCP client needs to access during boot is configured by default.

When multiple boot servers are defined, the first defined boot server has the highest priority. A DHCP client selects the next boot server only when it fails to communicate with the first defined boot server.

(5) (Optional) Configure the boot file name for a DHCP client.

bootfile *file-name*

No boot file name is configured for a DHCP client by default.

1.3.8 Assigning IP Addresses Based on Class Rules

1. Overview

In DHCP relay scenarios, addresses in a DHCP address pool can be assigned based on Option 82. When clients apply for IP addresses through different access points (APs), Option 82 carried in packets of the clients may be different. After class rules are configured on a DHCP server, the DHCP server can assign IP addresses in different network segments to clients based on Option 82 carried in the packets of the clients.

During address assignment, a DHCP server first determines an available address pool based on the network segment of a client. Then, it determines the class of the client based on Option 82, and assigns an IP address from the network segment corresponding to the class. When a request packet matches multiple classes in the address pool, the DHCP server assigns an IP address from the network segments corresponding to the classes based on the class configuration sequence. If the number of assigned IP addresses of a class reaches the limit, the DHCP server assigns an IP address based on the next matching class.

2. Restrictions and Guidelines

A DHCP address pool can be associated with multiple classes.

Each class corresponds to one network segment. Network segments are assigned in ascending order, and the network segments of multiple classes can overlap. If a class is associated with an address pool but no network

segment is configured for the class, the default network segment of the class is the same as the network segment of the address pool.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a class rule and enter the class configuration mode.

ip dhcp class *class-name*

No class rule is configured by default.

(4) (Optional) Configure identification information for a class.

remark *class-remark*

No identification information is configured for a class by default.

(5) Enter the Option 82 information configuration mode.

relay agent information

(6) Configure an Option 82 information matching rule for a class.

relay-information hex *hex-string* [*]

No Option 82 matching rule is configured by default.

(7) Return to the global configuration mode.

exit

(8) Enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(9) Associate an address pool with a class.

class *class-name*

No class is associated with a DHCP address pool by default.

(10) (Optional) Configure the IP address range corresponding to a class rule.

address range *low-ip-address high-ip-address*

The IP address range corresponding to a class rule is the network segment of the associated address pool by default.

(11) Return to the global configuration mode.

exit

(12) Enable address assignment based on class rules.

ip dhcp use class

Address assignment based on class rules is not configured by default.

1.3.9 Assigning IP Addresses Based on AM Rules

1. Overview

In super VLAN scenarios, address management (AM) rules can be used to plan IP address ranges for DHCP clients in different VLANs or DHCP clients using different ports, so that IP addresses can be assigned effectively and more flexibly. After an AM rule is configured, all DHCP clients from the specified VLANs and ports can obtain IP addresses. If a DHCP client is from a VLAN or port that is not specified, there are two cases: If a default AM rule is configured, the client obtains an IP address from the default IP address range; if no default AM rule is configured, the client cannot obtain an IP address.

2. Restrictions and Guidelines

This function can be configured only on Ethernet, Frame Relay (FR), Point-to-Point Protocol (PPP), or High-level Data Link Control (HDLC) interfaces.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the AM rule configuration mode.

address-manage

(4) Configure an AM rule. Select at least one of the following configuration steps.

- Configure the default IP address range matched with an AM rule.

  match ip default *ip-address netmask*

- Configure dynamic address assignment based on the VLAN and port.

  match ip *ip-address netmask* [*interface-type interface-number*] [**add | remove**] **vlan** *vlan-id*

- Configure static address assignment based on the VLAN.

  match ip *ip-address netmask* [**add** | **remove**] **vlan** *vlan-id*

No AM matching rule is configured by default.

(5) (Optional) Configure the loose mode for an AM rule.

match ip loose

The loose mode of AM rules is disabled by default.

If the loose mode is configured, clients that match no AM rule can obtain IP addresses in the way same as the case with no AM rule configured.

1.3.10 Refreshing Trusted ARP Entries

1. Overview

Trusted ARP entries protect a gateway from ARP spoofing. Ruijie devices with DHCP enabled provide a configuration command to determine whether trusted ARP entries are delivered during address assignment. After the function of adding trusted ARP entries is configured, a DHCP server adds trusted ARP entries during

address assignment to prevent ARP spoofing. A trusted ARP entry has a higher priority than a dynamic ARP entry and is not overridden by the dynamic ARP entry.

After the function of refreshing trusted ARP entries is configured, a DHCP server refreshes trusted ARP entries only for clients assigned with addresses from an address pool that is configured with the **update arp** command.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Refresh trusted ARP entries.

ip dhcp refresh arp

1.3.11 Configuring Rogue DHCP Server Detection

1. Overview

If a DHCP server is deployed illegally, when clients request IP addresses from this server, clients are assigned with wrong addresses. This server is a rogue server. Ruijie devices with DHCP enabled provide a command to enable rogue server detection. After rogue server detection is enabled, DHCP packets are checked for Option 54 (**Server Identifier**). If Option 54 is carried and its value is different from the actual DHCP server identifier, the IP address of the rogue server and the port receiving the packets are recorded. Rogue server detection is only a post-event detection function for security and cannot prevent an illegal DHCP server from assigning IP addresses to clients.

After rogue server detection is configured, rogue servers in a network are recorded into logs.

2. Procedure

(2) Enter the privileged EXEC mode.

enable

(3) Enter the global configuration mode.

configure terminal

(1) Configure rogue server detection.

ip dhcp server detect

Rogue server detection is disabled by default.

1.3.12 Configuring IP Address Conflict Detection

1. Overview

An excluded address is an IP address or address segment excluded from the address pool of a DHCP server, so that the DHCP server does not assign this IP address or address segment to a client. Excluding IP addresses can improve the address assignment efficiency.

When the DHCP server attempts to assign an IP address from the address pool, it uses the ping operation to check whether the IP address is occupied by another host. If yes, the DHCP server records the IP address. If not, the DHCP server assigns the IP address to a DHCP client.

The ARP entry check function can be used with the ping operation to detect IP address conflicts. If a client is configured with a static IP address and Layer 2 isolation is configured in an environment and the ping operation for IP address conflict detection becomes invalid (for example, a firewall is enabled on the client), this IP address may be assigned to another client that dynamically requests an address, resulting in an IP address conflict.

2. Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring Excluded IP Addresses
- Configuring the Number of Ping Operations Executed for Address Conflict Detection
- Configuring the Timeout Time of a Ping Operation Executed for Address Conflict Detection
- Configuring ARP Entry Check

3. Configuring Excluded IP Addresses

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure excluded IP addresses.

ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

No excluded IP address is configured by default. A DHCP server assigns all addresses from an IP address pool to DHCP clients.

4. Configuring the Number of Ping Operations Executed for Address Conflict Detection

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the number of ping operations executed by a DHCP server when it detects IP address conflicts.

ip dhcp ping packets [*ping-times*]

A DHCP server pings a conflicted IP address two times by default.

5. Configuring the Timeout Time of a Ping Operation Executed for Address Conflict Detection

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the timeout time of a ping operation executed when a DHCP server detects address conflicts.

ip dhcp ping timeout *time*

The default timeout time of a ping operation for detecting address conflicts is 500 ms.

6. Configuring ARP Entry Check

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the ARP entry check.

ip dhcp arp-probe

The ARP entry check is disabled by default.

1.3.13 Configuring Compulsory NAK Reply

1. Overview

When a DHCP client moves from another network to the local network, the DHCP server does not reply with a NAK packet because it cannot find the corresponding lease record locally. In this case, the DHCP client needs to send REQUEST packets repeatedly. The client can obtain an IP address again only when the request times out, and the time for obtaining an IP address is lengthened. This case also occurs when a client requires lease renewal but the DHCP server loses the lease record of the client due to a restart. In this case, you can configure compulsory NAK reply for the DHCP server if no lease record is found, so as to ensure that the client can obtain an IP address quickly.

2. Restrictions and Guidelines

When compulsory NAK reply is enabled, enable only one DHCP server in a broadcast domain. Configuring compulsory NAK reply may cause exceptions to other servers.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure compulsory NAK reply for a DHCP server.

ip dhcp force-send-nak

Compulsory NAK reply is enabled by default.

1.3.14 Configuring VRRP Monitoring

1. Overview

After VRRP monitoring is enabled in VRRP application scenarios, only the master server processes DHCP packets.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the Layer 3 interface configuration mode.

interface *interface-type interface-number*

(4) Enable VRRP monitoring.

ip dhcp monitor-vrrp-state

VRRP monitoring is disabled for an interface by default.

1.3.15 Configuring ARP-based Go-Offline Detection

1. Overview

Ruijie devices with DHCP enabled provide a command to enable ARP-based go-offline detection. After this function is enabled, a DHCP server receives an ARP entry aging notification when a client goes offline, and reclaims the client's IP address. If the client does not go online within a period of time (5 minutes by default), the DHCP server reclaims the IP address and assigns it to another client. If the client goes online again within the specified period, it can still use the original IP address.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure ARP-based go-offline detection.

ip dhcp server arp-detect

ARP-based go-offline detection is not configured for a DHCP server by default.

1.3.16 Saving Historical Leases

1. Overview

After a DHCP server assigns an IP address to a client and the client goes offline, the DHCP server saves the IP address lease of the client to the database. When the client goes online again, the DHCP server assigns this address to the client again. Historical leases are saved when a DHCP process restarts or the device performs a hot backup switchover.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of saving historical leases.

ip dhcp save-history-enable

The function of saving historical leases is disabled by default.

1.4 Configuring DHCP Relay

1.4.1 Overview

When a DHCP client and a DHCP server are in different network segments, a DHCP relay agent is required for dynamic IP address management.

1.4.2 Configuration Task Summary

(1) Configuring Basic DHCP Relay Functions

(2) Configuring extended DHCP relay functions: All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring Option 82
- Configuring Server-ID Check
- Enabling DHCP Relay Suppression
- Configuring Multiple Gateway IP Addresses
- Forcing a DHCP Relay to Send a Reply Packet
- Configuring the Source IP Address of DHCP Relay Packets

1.4.3 Configuring Basic DHCP Relay Functions

1. Overview

Generally, the DHCP relay function is implemented by an interface. The IP address of the server should be specified on the DHCP relay agent. In this case, DHCP broadcast packets received over this interface are sent to the specified server.

2. Restrictions and Guidelines

To enable DHCP relay, configure IPv4 unicast routing in a network.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the DHCP relay function.

service dhcp

The DHCP relay function is disabled by default.

(4) Configure the IP address of the DHCP server.

ip helper-address { **cycle-mode** | [**vrf** *vrf-name*] *ip-address* }

The IP address of the DHCP server is not configured for the DHCP relay agent by default.

The DHCP server address can be globally configured or configured on an Layer 3 interface. A maximum of 20 DHCP server addresses can be globally configured or configured on each Layer 3 interface. When an interface receives a DHCP request packet, the DHCP server list on the interface prevails over that

configured globally. If the interface is not configured with the DHCP server list, the global DHCP server list takes effect.

1.4.4 Configuring Option 82

1. Overview

A DHCP relay agent can use Option 82 to identify network information of DHCP clients, so that a DHCP server can assign IP addresses of different privileges to the clients more accurately based on this option.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Option 82.

ip dhcp relay information option82

DHCP Option 82 is disabled by default.

(4) Configure sub-options of DHCP Option 82. All the configuration steps below are optional. Select configuration steps as required.

- Customize information in **Circuit ID**.

  ip dhcp relay information option82 user-defined circuit-id *circuit-id-text*

  No custom information is configured for **Circuit ID** of DHCP Option 82 by default.

- Customize information in **Remote ID**.

  ip dhcp relay information option82 user-defined remote-id *remote-id-text*

  No custom information is configured for **Remote ID** of DHCP Option 82 by default.

(5) (Optional) Customize the MAC address format.

ip dhcp relay information option82 user-defined mac-format *mac-format-type*

The default MAC address format is H.H.H.

1.4.5 Configuring Server-ID Check

1. Overview

In a DHCP relay application environment, multiple DHCP servers are configured in each network to provide server backup, thereby helping ensure uninterrupted network operation. When a DHCP client has selected a DHCP server to send a DHCP REQUEST packet, a **Server-ID** option is carried in the packet. To reduce server load in specific environments, enable the **Server-ID** check function on the DHCP relay agent, so as to send the DHCP REQUEST packet only to the DHCP server specified in this option.

In this case, the DHCP relay agent sends DHCP request packets only to the specified server. If this function is not configured, the DHCP relay agent sends DHCP request packets to all configured DHCP servers.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable a DHCP relay agent to check **Server-ID**.

ip dhcp relay check server-id

The **Server-ID** check function is disabled by default.

1.4.6 Enabling DHCP Relay Suppression

1. Overview

After you enable DHCP relay suppression on an interface, DHCP request packets received over the interface are filtered out, but the other DHCP requests are forwarded.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the DHCP relay suppression function.

ip dhcp relay suppression

The DHCP relay suppression function is disabled on all interfaces by default.

1.4.7 Configuring Multiple Gateway IP Addresses

1. Overview

After the function of configuring multiple gateway IP addresses is enabled, a DHCP relay agent can use multiple interface IP addresses to send address requests to a DHCP server. Generally, the primary IP address is used as the gateway IP address, and the DHCP server assigns a network segment based on the gateway IP address. When a client fails to apply for an IP address through the gateway by using the primary IP address, it applies for an IP address through the gateway by using a secondary IP address.

After the automatic gateway switchover function is enabled, the DHCP relay agent adds another address to the **giaddr** field if it does not receive a reply for three consecutive DISCOVER packets.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of configuring multiple gateway IP addresses on a DHCP relay agent.

ip dhcp relay multiple-giaddr

The function of configuring multiple gateway IP addresses on a DHCP relay agent is disabled by default.

(4) (Optional) Enable the automatic gateway switchover function.

ip dhcp smart-relay

The automatic gateway switchover function is disabled by default.

1.4.8 Forcing a DHCP Relay to Send a Reply Packet

1. Overview

After the function of forcing a DHCP relay agent to send a reply packet is enabled, a DHCP relay agent forcibly specifies a gateway interface to send a reply if it fails to find a MAC address egress. When the function is disabled, the DHCP relay agent discards packets if it fails to find a MAC address egress.

2. Restrictions and Guidelines

You must enable basic DHCP Relay functions.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of forcing a DHCP relay agent to send a reply packet.

ip dhcp relay force-send-reply-pack

The function of forcing a DHCP relay agent to send a reply packet is disabled by default.

1.4.9 Configuring the Source IP Address of DHCP Relay Packets

1. Overview

You can run the **ip dhcp relay source** command on an interface to configure the source IP address of DHCP relay packets.

2. Restrictions and Guidelines

- Only one source IP address can be specified for DHCP relay packets on each interface.
- To assign correct subnet addresses to clients, this function should be used with Option 82.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the source IP address for DHCP relay packets.

ip dhcp relay source *ip-address*

No source address is configured for DHCP relay packets by default.

1.5 Monitoring

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

Run the **debug** command to output debugging information.

Caution

The output of debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** command to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear ip dhcp binding { * | *ip-address* }	Clears DHCP address binding records.
clear ip dhcp conflict { * | *ip-address* }	Clears DHCP address conflict records.
clear ip dhcp history { * | *mac-address* }	Clears DHCP historical records.
clear ip dhcp server detect { * | *ip-address* }	Clears rogue DHCP server detection records.
clear ip dhcp server rate	Clears DHCP server performance statistics.
clear ip dhcp server statistics	Clears DHCP server statistics.
clear ip dhcp relay statistics	Clears DHCP relay statistics.
show ip dhcp binding	Displays DHCP address bindings.
show ip dhcp conflict	Displays address conflict records of a DHCP server.
show ip dhcp history	Displays DHCP historical lease records.
show ip dhcp identifier	Displays the address pool ID and address usage of a DHCP server.
show ip dhcp pool [*pool-name*]	Displays the address pool status and utilization of a DHCP server.
show ip dhcp relay-statistic	Displays DHCP relay statistics.
show ip dhcp server detect	Displays rogue DHCP server detection information.
show ip dhcp server statistic	Displays DHCP server statistics.

show ip dhcp socket	Displays DHCP socket indexes.
debug ip dhcp server agent	Debugs a DHCP server.
debug ip dhcp server ha	Debugs DHCP hot backup.
debug ip dhcp server pool	Debugs DHCP address pools.
debug ip dhcp server vrrp	Debugs association between a DHCP server and a VRRP group.
debug ip dhcp server all	Debugs all DHCP servers.
debug ip dhcp relay	Debugs a DHCP relay.

1.6 Configuration Examples

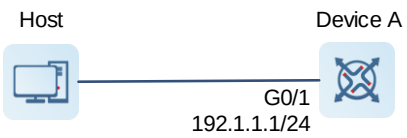
1.6.1 Configuring Static Address Binding

1. Requirements

As shown in Figure 1-16, a host that serves as a DHCP client obtains a statically bound IP address from Device A that serves as a DHCP server. The MAC address of the host is 0050.56b0.2f50.

2. Topology

Figure 1-16 Static Address Binding



3. Notes

Configure Device A:

- Configure the IP address of the interface.
- Enable the DHCP server service and configure address pool parameters.

4. Procedure

(1) Configure Device A:

Configure the IP address of the interface.

```
DeviceA> enable
DeviceA # configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.1.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Enable the DHCP server service.

```
DeviceA(config)# service dhcp
```

Create an address pool named **pool1**.

```
DeviceA(config)# ip dhcp pool pool1
```

Assign a statically bound IP address to the host.

```
DeviceA(dhcp-config)# host 192.1.1.99 255.255.255.0
DeviceA(dhcp-config)# hardware-address 0050.56b0.2f50
```

(2) Configure the host:

Enable DHCP on the host to obtain an IP address. (Omitted)

5. Verification

Check that the host has obtained the IP address 192.1.1.99/24.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 ip address 192.1.1.1 255.255.255.0
!
 service dhcp
!
 ip dhcp pool pool1
 host 192.1.1.99 255.255.255.0
 hardware-address 0050.56b0.2f50
!
```

7. Common Errors

- No address pool is configured.
- The DHCP Server service is not enabled.

1.6.2 Dynamically Assigning IP Addresses

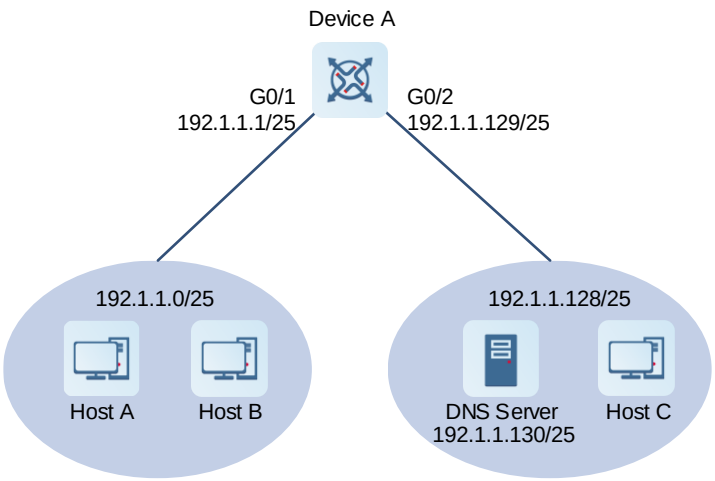
1. Requirements

As shown in Figure 1-17, Device A serving as a DHCP server dynamically assigns IP addresses to clients in the same network segment. The address pool is divided into two network segments: 192.1.1.0/25 and 192.1.1.128/25.

The lease time of IP addresses in network segment 192.1.1.0/25 is 5 days, the domain name suffix is **test.com**, the DNS address is 192.1.1.130, and the gateway address is 192.1.1.1. The lease time of IP addresses in network segment 10.1.1.128/25 is 3 days, the domain name suffix is **test.com**, the DNS address is 192.1.1.130, and the gateway address is 192.1.1.129.

2. Topology

Figure 1-17 Dynamically Assigning IP Addresses



3. Notes

Configure Device A:

- Configure the IP address of the interface for connecting to the host.
- Enable the DHCP Server service and configure parameters of two address pools.

4. Procedure

(1) Configure Device A:

Configure the IP address of the interface for connecting to the host.

```
DeviceA> enable
DeviceA # configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.1.1.1 255.255.255.128
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ip address 192.1.1.129 255.255.255.128
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

Enable the DHCP Server service.

```
DeviceA(config)# service dhcp
```

Configure network parameters of pool 1.

```
DeviceA(config)# ip dhcp pool pool1
DeviceA(dhcp-config)# network 192.1.1.0 255.255.255.128
DeviceA(dhcp-config)# default-router 192.1.1.1
DeviceA(dhcp-config)# dns-server 192.1.1.130
DeviceA(dhcp-config)# domain-name test.com
DeviceA(dhcp-config)# lease 5
DeviceA(dhcp-config)# exit
```

Configure network parameters of pool 2.

```
DeviceA(config)# ip dhcp pool pool2
DeviceA(dhcp-config)# network 192.1.1.128 255.255.255.128
DeviceA(dhcp-config)# default-router 192.1.1.129
DeviceA(dhcp-config)# dns-server 192.1.1.130
DeviceA(dhcp-config)# domain-name test.com
DeviceA(dhcp-config)# lease 3
```

(2) Configure the DNS server:

Set the DNS server IP address to 192.1.1.130/25. (Omitted)

(3) Configure the host:

Enable DHCP on Host A, Host B, and Host C to obtain IP addresses. (Omitted)

5. Verification

Check that Host A and Host B have obtained addresses in network segment 192.1.1.0/25.

Check that Host C has obtained an address in network segment 192.1.1.128/25.

Run the **show ip dhcp pool** command on Device A to display address pool configurations and usage.

```
DeviceA(config)# show ip dhcp pool
Pool  name      Total    Distributed  Remained   Percentage
------------  -----------  -----------  --------   -----------
pool1        126         2          124       0.98413
pool2        126         1          125       0.99206
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 ip address 192.1.1.1 255.255.255.128
!
 interface gigabitethernet 0/2
 ip address 192.1.1.129 255.255.255.128
!
 service dhcp
!
 ip dhcp pool pool1
 network 192.1.1.0 255.255.255.128
 default-router 192.1.1.1
 dns-server 192.1.1.130
 domain-name test.com
 lease 5
!
 ip dhcp pool pool2
 network 192.1.1.128 255.255.255.128
 default-router 192.1.1.129
```

```
 dns-server 192.1.1.130
 domain-name test.com
 lease 3
!
```

7. Common Errors

- No address pool is configured.
- The DHCP Server service is not enabled.

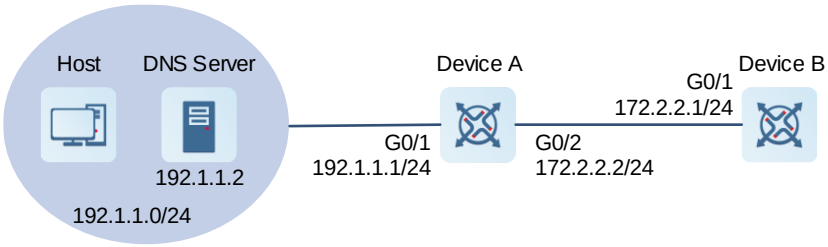
1.6.3 Configuring DHCP Relay

1. Requirements

As shown in Figure 1-18, a host serving as a DHCP client is located in network segment 192.1.1.0/24, Device A is the gateway, and Device B is a DHCP server. To apply for an IP address and other configurations from the DHCP server, the DHCP client needs to use the gateway as a DHCP relay agent, so that the DHCP relay agent forwards DHCP packets to the DHCP server.

2. Topology

Figure 1-18 Configuring DHCP Relay



3. Notes

- Configure Device A:
  - Configure the IP address of the interface.
  - Enable the DHCP relay function.
- Configure Device B:
  - Configure the IP address of the interface.
  - Configure a route from Device B to GigabitEthernet 0/1 on Device A.
  - Enable the DHCP server service and configure address pool parameters.

4. Procedure

(1) Configure Device A:

Configure the IP address of the interface.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.1.1.1 255.255.255.0
```

```
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

Enable the DHCP relay function.

```
DeviceA(config)# service dhcp
```

Add the DHCP server address to the DHCP relay agent.

```
DeviceA(config)# ip helper-address 172.2.2.1
```

(2) Configure Device B:

Configure the IP address of the interface.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 172.2.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure a static route to network segment 192.1.1.0/24.

```
DeviceB(config)# ip route 192.1.1.0 255.255.255.0 gigabitethernet 0/1
```

Enable the DHCP server function.

```
DeviceB(config)# service dhcp
```

Configure network parameters of pool 1.

```
DeviceB(config)# ip dhcp pool pool1
DeviceB(dhcp-config)# network 192.1.1.0 255.255.255.0
DeviceB(dhcp-config)# default-router 192.1.1.1
DeviceB(dhcp-config)# dns-server 192.1.1.2
DeviceB(dhcp-config)# exit
```

(3) Enable DHCP on the host to obtain an IP address. (Omitted)

5. Verification

Check that the host has obtained an address in network segment 192.1.1.0/24.

Run the **show ip dhcp pool** command on Device B to display the address pool configurations and usage.

```
DeviceB(config)# show ip dhcp pool
Pool  name      Total    Distributed  Remained   Percentage
------------  -----------  -----------  --------   -----------
pool1        126         1           125       0.99206
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 ip address 192.1.1.1 255.255.255.0
!
```

```
 interface gigabitethernet 0/2
!
 service dhcp
 ip helper-address 172.2.2.1
!
```

- Device B configuration file

```
hostname DeviceB
!
 interface gigabitethernet 0/1
 ip address 172.2.2.1 255.255.255.0
!
 ip route 192.1.1.0 255.255.255.0 gigabitethernet 0/1
 service dhcp
!
 ip dhcp pool pool1
 network 192.1.1.0 255.255.255.0
 default-router 192.1.1.1
 dns-server 192.1.1.2
!
```

7. Common Errors

- The DHCP relay function is disabled on the DHCP relay agent.
- No route is configured between the DHCP relay agent and DHCP server.
- The IP address of the DHCP server is configured on the DHCP relay agent.

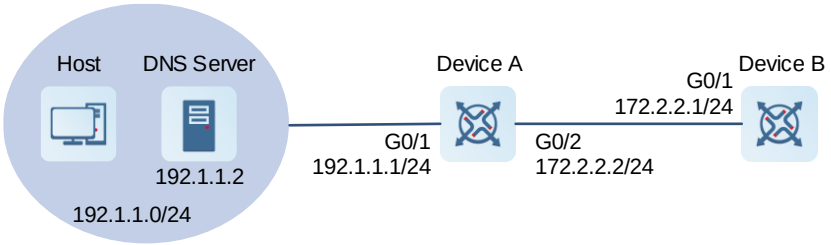
1.6.4 Assigning IP Addresses Based on Class Rules

1. Requirements

As shown in Figure 1-19, Device A serves as a DHCP server to assign IP addresses and other network configurations to clients, and Device B serves as a DHCP relay agent to forward DHCP packets between the clients and server. It is required that Device A assign an IP address in the range of 192.1.1.200 to 192.1.1.254 if a DHCP request packet carries Option 82 and assigns an IP address in the range of 192.1.1.1 to 192.1.1.199 if a DHCP request packet does not carry Option 82.

2. Topology

Figure 1-19 Assigning IP Addresses Based on Class Rules



3. Notes

- Configure Device A:
  - Configure the IP address of the interface.
  - Enable the DHCP relay function.
  - Enable the Option 82 function.
- Configure Device B:
  - Configure the IP address of the interface.
  - Configure a route from Device B to GigabitEthernet 0/1 on Device A.
  - Enable the DHCP server service and configure address pool parameters.
  - Add a specific class rule.

4. Procedure

(1) Configure Device A:

Configure the IP address of the interface.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.1.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

Enable the DHCP relay function.

```
DeviceA(config)# service dhcp
```

Add the DHCP server address.

```
DeviceA(config)# ip helper-address 172.2.2.1
```

Enable Option 82.

```
DeviceA(config)# ip dhcp relay information option82
```

(2) Configure Device B:

Configure the IP address of the interface.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 172.2.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure a static route to network segment 192.1.1.0/24.

```
DeviceB(config)# ip route 192.1.1.0 255.255.255.0 gigabitethernet 0/1
```

Enable the DHCP Server function.

```
DeviceB(config)# service dhcp
```

Configure a class rule.

```
DeviceB(config)# ip dhcp class myclass
DeviceB(config-dhcp-class)# relay agent information
DeviceB(config-dhcp-class-relayinfo)# relay-information hex 060223*
```

Create an address pool and configure related network parameters.

```
DeviceB(config)# ip dhcp pool pool1
DeviceB(dhcp-config)# network 192.1.1.0 255.255.255.0
DeviceB(dhcp-config)# default-router 192.1.1.1
DeviceB(dhcp-config)# dns-server 192.1.1.2
```

Configure the network segment for assigning an IP address when a class is matched.

```
DeviceB(dhcp-config)# class myclass
DeviceB(config-dhcp-pool-class)# address range 192.1.1.200 192.1.1.254
DeviceB(config-dhcp-pool-class)# exit
```

(3) Enable DHCP on the host to obtain an IP address. (Omitted)

5. Verification

Capture packets on Device B and check that clients that match Option 82 rules in a class rule have obtained IP addresses in the range of 192.1.1.200 to 192.1.1.254 and clients that do not match Option 82 rules in the class rule have obtained IP addresses in the range of 192.1.1.1 to 192.1.1.199.

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
 service dhcp
 ip helper-address 172.2.2.1
 ip dhcp relay information option82
!
 interface gigabitethernet 0/1
 ip address 192.1.1.1 255.255.255.0
 exit
 interface gigabitethernet 0/2
 ip address 172.2.2.2 255.255.255.0
!
```

- Device B configuration file

```
hostname DeviceB
!
 ip route 192.1.1.0 255.255.255.0 gigabitethernet 0/1
 service dhcp
!
 interface gigabitethernet 0/1
 ip address 172.2.2.1 255.255.255.0
!
 ip dhcp class myclass
 relay agent information
```

```
 relay-information hex 060223*
!
 ip dhcp pool pool1
 network 192.1.1.0 255.255.255.0
 default-router 192.1.1.1
 dns-server 192.1.1.2
 class myclass
   address range 192.1.1.200 192.1.1.254
!
```

7. Common Errors

- The DHCP Relay function is disabled.
- No route is configured between the DHCP relay agent and DHCP server.
- No DHCP server IP address is configured.

Contents

1 Configuring DHCP Client 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 2
1.2 Enabling DHCP Client Function 2
1.2.1 Overview 2
1.2.2 Restrictions and Guidelines 2
1.2.3 Procedure 2
1.3 Monitoring 2
1.4 Configuration Examples 3
1.4.1 Enabling DHCP Client Function 3

1 Configuring DHCP Client

1.1 Introduction

1.1.1 Overview

Dynamic Host Configuration Protocol (DHCP) is a local area network (LAN) protocol based on the User Datagram Protocol (UDP) for dynamically assigning reusable network resources over port 68, for example, IP addresses.

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

1.1.2 Principles

1. DHCP client

A DHCP client enables a device to automatically obtain an IP address and other configurations from a DHCP server.

For details about interaction between the DHCP client and server, see *Configuring DHCP*.

2. Lease renewal

Generally, a dynamic IP address assigned from a DHCP server to a DHCP client has a lease period (one day by default). After the lease period expires, the DHCP server will reclaim this IP address. If the DHCP client wants to continue to use this IP address, it automatically sends a DHCP REQUEST packet to the DHCP server at half of the lease period to renew the lease. If this IP address is valid, the DHCP server returns a DHCP ACK packet to inform the DHCP client that it has obtained a new IP address lease.

If the lease renewal operation performed at half of the lease period fails (for example, the DHCP server does not make a response), the DHCP client broadcasts another DHCP REQUEST packet at 7/8 of the lease period to renew the lease. The DHCP server renews the lease in the same way.

3. Network reconnection

When a DHCP client reconnects to the network after it goes offline, it does not need to send a DHCP DISCOVER packet but only broadcasts a DHCP REQUEST packet that carries the previously assigned IP address.

After receiving the DHCP REQUEST packet, the DHCP server returns a DHCP ACK packet to inform the DHCP client that it can continue to use the original IP address if this IP address is not assigned. If the original IP address has been assigned to another client, the DHCP server returns a DHCP NAK packet. Upon receiving the DHCP NAK packet, the DHCP client needs to re-send a DHCP DISCOVER packet to apply for a new IP address.

4. Lease release

When a DHCP client no longer needs to use the assigned IP address, it can send a DHCP RELEASE packet to inform the DHCP server, for the DHCP server to release the DHCP lease and reclaim the IP address. The

DHCP server saves the configuration information of the DHCP client temporarily for reuse in next IP address application by the DHCP client.

1.1.3 Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 3046: DHCP Relay Agent Information Option
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol

1.2 Enabling DHCP Client Function

1.2.1 Overview

After the DHCP Client function is enabled on a device, the device can dynamically obtain IP addresses and other configurations, such as the default gateway and Domain Name System (DNS) server.

1.2.2 Restrictions and Guidelines

The device supports DHCP client configurations on Ethernet, Frame Relay (FR), Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC) interfaces.

1.2.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the DHCP Client function on an interface.

ip address dhcp

No interface can obtain an IP address through DHCP by default.

1.3 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** commands to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
show dhcp lease	Displays lease information of a DHCP client.
debug ip dhcp client	Debugs DHCP packets.

1.4 Configuration Examples

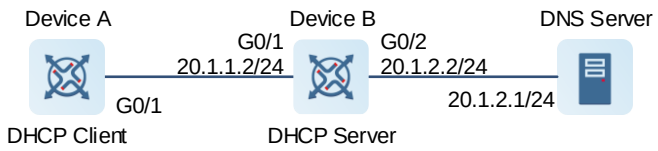
1.4.1 Enabling DHCP Client Function

1. Requirements

As shown in Figure 1-1, GigabitEthernet 0/1 on Device A uses DHCP to obtain an IP address and DNS server address 20.1.1.1/24 from Device B (DHCP server).

2. Topology

Figure 1-1 DHCP Client Function



3. Notes

- Enable the DHCP Client function on GigabitEthernet 0/1 of Device A.
- Enable the DHCP Server function on Device B and configure address pool parameters as required.

4. Procedure

(1) Configure Device A:

Enable the DHCP Client service on GigabitEthernet 0/1.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address dhcp
```

(2) Configure Device B:

Enable the DHCP Server service.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# service dhcp
```

Configure the interface IP address used to connect to the DHCP client.

```
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 20.1.1.2 255.255.255.0
```

```
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure the interface IP address used to connect to the DNS server.

```
DeviceB(config)# interface gigabitethernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# ip address 20.1.2.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/2)# exit
```

Configure a dynamic address pool.

```
DeviceB(config)# ip dhcp pool User
DeviceB(dhcp-config)# network 20.1.1.0 255.255.255.0
DeviceB(dhcp-config)# dns-server 20.1.2.1
DeviceB(dhcp-config)# exit
```

Configure excluded IP addresses.

```
DeviceB(config)# ip dhcp excluded-address 20.1.1.2
```

(3) Configure the DNS server:

Set the DNS server IP address to 20.1.2.1/24. (Omitted)

5. Verification

Run the **show dhcp lease** command on Device B to display the IP address information obtained from an interface.

```
DeviceB# show dhcp lease
Temp IP addr: 20.1.1.1  for peer on Interface: GigabitEthernet 0/1
Temp  sub net mask: 255.255.255.0
   DHCP Lease server: 20.1.1.2, state: 7 Bound
   DHCP transaction id: ca811331
   Lease: 14400 secs,  Renewal: 7200 secs,  Rebind: 12600 secs
   Next timer fires after: 4916 secs
   Retry count: 0   Client-ID: 0158696cc59347
```

Run the **show hosts** command on Device A to display DNS server information obtained from an interface.

```
DeviceA# show hosts
Name servers are:
20.1.2.1 dynamic from DHCP
Host                                 type    Address              TTL(sec)
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 ip address dhcp
!
```

- Device B configuration file

```
hostname DeviceB
!
 service dhcp
```

```
 ip dhcp excluded-address 20.1.1.2
!
 interface gigabitethernet 0/1
 ip address 20.1.1.2 255.255.255.0
!
 interface gigabitethernet 0/2
 ip address 20.1.2.2 255.255.255.0
!
 ip dhcp pool User
 network 20.1.1.0 255.255.255.0
 dns-server 20.1.2.1
!
```

Contents

1 Configuring DHCP Snooping 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Applications 3
1.1.4 Protocols and Standards 6
1.2 Restrictions and Guidelines 6
1.3 Configuration Task Summary 7
1.4 Configuring Basic DHCP Snooping Functions 7
1.4.1 Overview 7
1.4.2 Procedure 7
1.5 Disabling DHCP Snooping on a VLAN 8
1.6 Enabling Source MAC Address Verification 8
1.6.1 Overview 8
1.6.2 Procedure 8
1.7 Writing Dynamic User Information in the DHCP Snooping Binding Database to the Flash Memory in Real Time 8
1.8 Writing Dynamic User Information in the DHCP Snooping Binding Database to a Flash Memory at a Scheduled Time 9
1.9 Enabling DHCP Snooping to Support BOOTP Binding 9
1.10 Enabling DHCP Snooping to Support Relay Request Packet Processing 9
1.11 Enabling DHCP Snooping to Support Binding Entry Migration 10
1.12 Enabling DHCP Snooping to Fast Age Client Migration Entries 10

1.13 Configuring an Interface in the Suppression State 10

1.14 Configuring the Maximum Number of Users Bound to a VLAN 10

1.15 Configuring Option 82 11

1.15.1 Overview 11

1.15.2 Restrictions and Guidelines 11

1.15.3 Procedure 11

1.16 Enabling DHCP Snooping Monitoring 12

1.16.1 Overview 12

1.16.2 Restrictions and Guidelines 12

1.16.3 Procedure 12

1.17 Monitoring 12

1.18 Configuration Examples 13

1.18.1 Configuring DHCP Snooping 13

1.19 Common Misconfigurations 14

1 Configuring DHCP Snooping

1.1 Introduction

1.1.1 Overview

The Dynamic Host Configuration Protocol (DHCP) snooping function allows a device to snoop DHCP packets exchanged between clients and a server to record and monitor the IP address usage and filter out invalid DHCP packets, including request packets from the clients and response packets from the server. User data entries generated from DHCP Snooping records may serve security applications such as IP Source Guard.

1.1.2 Principles

1. Basic Concepts

- DHCP request packets

  Request packets are sent from a DHCP client to a DHCP server, including DHCP DISCOVER, DHCP REQUEST, DHCP DECLINE, DHCP RELEASE, and DHCP INFORM packets.

- DHCP response packets

  Response packets are sent from a DHCP server to a DHCP client, including DHCP OFFER, DHCP ACK, and DHCP NAK packets.

- VLAN-based DHCP Snooping

  DHCP Snooping is enabled on a per-VLAN basis. When DHCP Snooping is enabled on a device, it is effective to all VLANs of the device by default. You can flexibly configure the VLANs on which DHCP Snooping is enabled.

- DHCP Snooping trusted ports

  Packet for obtaining IP addresses through DHCP are exchanged via broadcast. Rough DHCP services affect clients' normal acquisition of IP addresses and lead to user information spoofing and stealing. DHCP Snooping ports are classified into trusted ports and untrusted ports to prevent rough DHCP services.

  The device only transmits DHCP response packets received on trusted ports and discards those received from untrusted ports. In this way, the ports connected to legitimate DHCP servers are configured as trusted ports and the other ports are configured as untrusted ports to shield rough DHCP servers.

  On switches, all switching ports or L2 aggregation ports (APs) are defaulted as untrusted, and trusted ports can be specified.

- DHCP Snooping binding database

  In a DHCP network, clients may set static IP addresses randomly. This increases not only the difficulty of network maintenance but also the possibility that legitimate clients with IP addresses assigned by a DHCP server may fail to use the network due to address conflicts. By snooping packets between the clients and server, DHCP Snooping summarizes user entries, including IP addresses, media access control (MAC) addresses, VLAN IDs (VIDs), ports, and lease time to build the DHCP Snooping binding database. Combined with Address Resolution Protocol (ARP) detection or ARP check, DHCP Snooping controls the reliable assignment of IP addresses to legitimate clients.

- DHCP Snooping packet suppression

  To shield all the DHCP packets on a specific client, enable DHCP Snooping packet suppression on its untrusted ports.

- DHCP Snooping rate limit

  DHCP Snooping rate limit can be configured using the rate limit command of Network Foundation Protection Policy (NFPP). For NFPP configuration, see "Configuring NFPP" in the *Security Configuration Guide*.

- DHCP Option 82

  DHCP Option 82, also called the DHCP relay agent information option, is an option in DHCP packets. Option 82 is used to enhance the DHCP server security and optimize the IP address assignment policy. This option is usually configured on the DHCP relay service component, such as DHCP Relay and DHCP Snooping of a network access device. This option is transparent to clients and added or removed by the DHCP relay component.

- Invalid DHCP packets

  The device with DHCP Snooping enabled checks validity of received DHCP packets, discards invalid DHCP packets, and records information about legitimate users to form the DHCP Snooping binding database for query by other applications (for example, ARP detection). The following types of packets are considered as invalid DHCP packets:

  - DHCP response packets received on untrusted ports, including DHCP ACK, DHCP NAK, and DHCP OFFER packets
  - DHCP request packets carrying the **giaddr** field (gateway information) received on untrusted ports
  - Packets with the source MAC addresses different from the value of the **chaddr** field in DHCP packets in a case with MAC address verification enabled
  - DHCP RELEASE packets corresponding to entries in the DHCP Snooping binding database, with the untrusted port on which the packets are received being inconsistent with the untrusted port in the binding table
  - DHCP packets in incorrect formats or incomplete DHCP packets

2. Filtering Invalid DHCP Packets

The device with DHCP Snooping enabled checks validity of DHCP packets from untrusted ports to control the transmission scope of the packets and prevent spoofing.

During snooping, it checks the receiving ports and fields of packets to filter packets, and modifies the destination ports of the packets to control the packet transmission scope.

- Checking ports

  When receiving a DHCP packet, the device first checks whether the port receiving the packet is a DHCP trusted port. If yes, the device directly forwards the packet without checking the validity or generating a binding record. If not, the device checks its validity.

- Checking packet encapsulation and length

  The device checks whether received packets are UDP packets, whether the destination port is port 67 or 68, and whether the packet length matches the length field defined in protocols.

- Checking packet fields and types

According to the invalid DHCP packet types introduced in the "Basic Concepts" section, the device first checks the **giaddr** and **chaddr** fields in packets and then checks whether the restrictive conditions for this packet type are met.

3. Building a DHCP Snooping Binding Database

The device with DHCP Snooping enabled detects packets exchanged between the DHCP clients and the DHCP server and generates entries in the DHCP Snooping binding database based on information about valid DHCP packets. All these entries are used as the information table of legitimate users, and provided to other security modules of the device as the basis for filtering network packets.

The binding database is updated during snooping based on the types of DHCP packets.

- Generating binding entries

  When a DHCP ACK packet is snooped on a trusted port, the device with DHCP Snooping enabled extracts the client's IP address, MAC address, and lease time from the packet and generates a binding entry based on the recorded port ID (interface index) and VLAN ID of the client.

- Deleting binding entries

  A binding entry is deleted in the following scenarios:

  - The recorded lease time expires.
  - A valid DHCP RELEASE or DHCP DECLINE packet sent from the client is snooped.
  - A NAK packet is received from a trusted port.
  - A user runs the **clear** command to delete a binding entry.

1.1.3 Applications

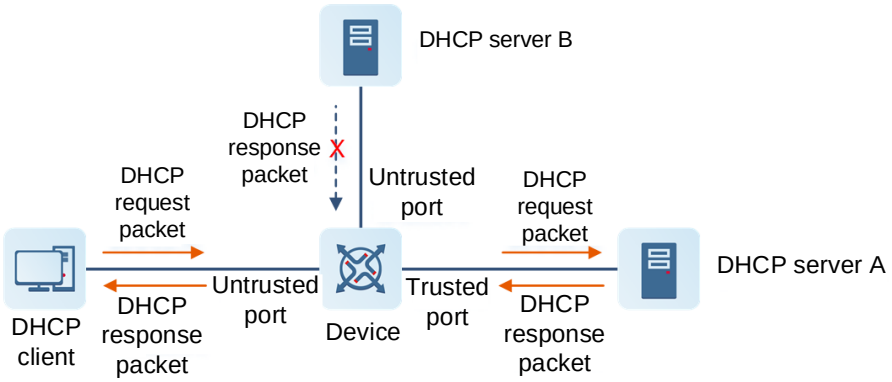
1. Guarding Against DHCP Spoofing

Multiple DHCP servers may exist in a network. It is essential to ensure that PCs can obtain network configurations only from the DHCP servers within a controlled area.

As shown in the following figure, the DHCP client can communicate with a trusted DHCP server only.

- Request packets from the DHCP client are transmitted only to the trusted DHCP server.
- Only response packets from the trusted DHCP server can be transmitted to the DHCP client.

Figure 1-1 Guarding Against DHCP Spoofing



Device is an access device, DHCP Server A is in the controlled area, and DHCP Server B is beyond the controlled area.

- DHCP Snooping is enabled on Device to monitor DHCP packets.
- The port on Device for connecting to DHCP Server A is configured as a DHCP trusted port to forward response packets.
- The rest of ports on Device are configured as DHCP untrusted ports to filter response packets.

2. Guarding Against DHCP Packet Flooding

Malicious DHCP clients in a network may send DHCP packets at a high rate. As a result, legitimate users cannot obtain IP addresses, and access devices are heavily loaded or even break down.

- To ensure network stability, the DHCP Snooping rate limit function needs to be enabled for DHCP packets. The request packets from DHCP clients are sent at a rate below the limit. Packets sent at rates beyond the limit are discarded. DHCP Snooping is correlated with the ARP module to delete entries of non-existing users.

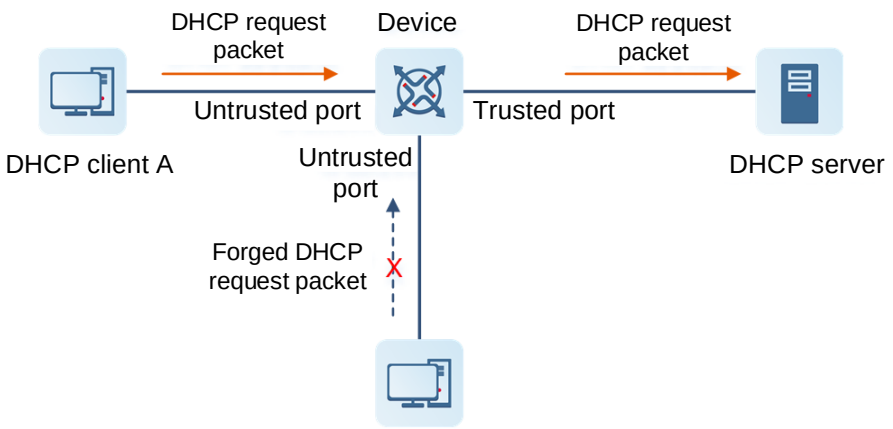
3. Guarding Against Forged DHCP Packets

Malicious DHCP clients in a network may forge DHCP request packets, which consumes applicable IP addresses from the servers and probably preempts legitimate users' IP addresses. Therefore, it is necessary to filter out invalid DHCP packets.

As shown in the following figure, the DHCP request packets sent from DHCP clients are checked.

- The source MAC address field in request packets from DHCP clients must match the client hardware address field of the DHCP packets.
- The RELEASE and DECLINE packets from clients must match the entries in the DHCPv6 Snooping binding database.

Figure 1-2 Guarding Against Forged DHCP Packets



Device is an access device, and DHCP Server is in the controlled area.

- DHCP Snooping is enabled on Device to monitor DHCP packets.
- The port on Device for connecting to DHCP Server is configured as a DHCP trusted port to forward

response packets.

- The rest of ports on Device are configured as DHCP untrusted ports to filter response packets.
- DHCP source MAC addresses need to be verified on untrusted ports of Device to filter out invalid DHCP packets.

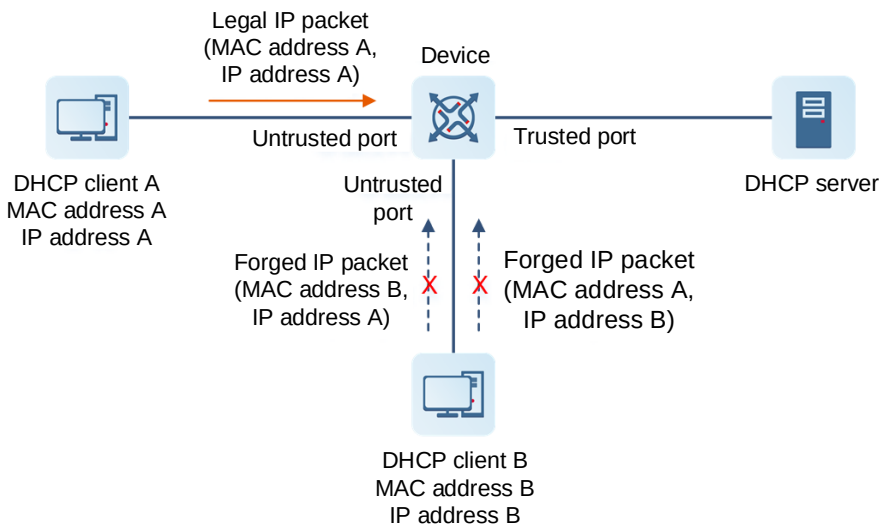
4. Guarding Against IP/MAC Address Spoofing

You can check IP packets from untrusted ports based the IP address field or IP address and MAC address fields to filter out forged IP packets.

As shown in the following figure, IP packets sent from DHCP clients are checked.

- The source address field in IP packets must match the IP address assigned by the DHCP server.
- The source MAC address field in L2 packets must match the client hardware address field in DHCP request packets from clients.

Figure 1-3 Guarding Against IP/MAC Address Spoofing



Device is an access device, and DHCP Server is in the controlled area.

- DHCP Snooping is enabled on Device to monitor DHCP packets.
- The port on Device for connecting to DHCP Server is configured as a DHCP trusted port.
- All downlink ports on Device are configured as DHCP untrusted ports.
- IP Source Guard is enabled on Device to filter IP packets.
- The IP Source Guard matching mode is set to IP+MAC on Device to check the MAC address and IP address fields in IP packets.

5. Preventing Private IP Addresses

The device with DHCP Snooping enabled checks whether the source addresses in IP packets from untrusted ports are consistent with the IP addresses assigned by the DHCP server.

If the source addresses, connected ports, and L2 source MAC addresses in IP packets do not match the assignments of the DHCP server, such packets are discarded.

The working process of the device in this scenario is the same as that in "Guarding Against IP/MAC Address Spoofing".

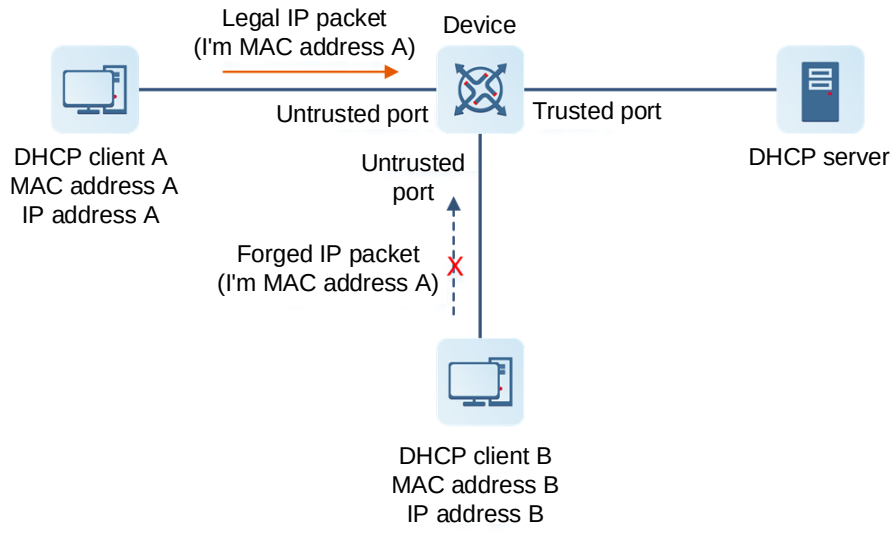
6. Detecting ARP Attacks

The device with DHCP Snooping enabled checks the ARP packets from untrusted ports and filter out the ARP packets unmatched with the assignments of the DHCP server.

As shown in the following figure, ARP packets sent from DHCP clients are checked.

The ports receiving ARP packets, the L2 MAC addresses, and the hardware addresses of ARP packet senders must be consistent with the snooped DHCP packet records.

Figure 1-4 Detecting ARP Attacks



Device is an access device, and DHCP Server is in the controlled area.

- DHCP Snooping is enabled on Device to monitor DHCP packets.
- The port on Device for connecting to DHCP Server is configured as a DHCP trusted port.
- All downlink ports on Device are configured as DHCP untrusted ports.
- IP Source Guard and ARP check are enabled on all untrusted ports on Device to filter ARP packets.

1.1.4 Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions

1.2 Restrictions and Guidelines

- All security control functions are effective only to DHCP untrusted ports.
- The ports on the device for connecting to trusted DHCP servers must be configured as DHCP trusted ports.
- DHCP Snooping takes effect to switching ports, L2 APs, and L2 encapsulation sub-interfaces.
- DHCP Snooping and DHCP Relay are mutually exclusive in virtual routing and forwarding (VRF) scenarios.

1.3 Configuration Task Summary

DHCP Snooping configuration includes the following tasks:

The following configuration tasks are mutually exclusive. Please configure only one task.

- Configuring DHCP Snooping
  - a Configuring Basic DHCP Snooping Functions
  - b (Optional) Disabling DHCP Snooping on a VLAN
  - c (Optional) Enabling Source MAC Address Verification
  - d (Optional) Writing Dynamic User Information in the DHCP Snooping Binding Database to the Flash Memory in Real Time
  - e (Optional) Writing Dynamic User Information in the DHCP Snooping Binding Database to a Flash Memory at a Scheduled Time
  - f (Optional) Enabling DHCP Snooping to Support BOOTP Binding
  - g (Optional) Enabling DHCP Snooping to Support Relay Request Packet Processing
  - h (Optional) Enabling DHCP Snooping to Support Binding Entry Migration
  - i (Optional) Enabling DHCP Snooping to Fast Age Client Migration Entries
  - j (Optional) Configuring an Interface in the Suppression State
  - k (Optional) Configuring the Maximum Number of Users Bound to a VLAN
  - l (Optional) Configuring Option 82
- Enabling DHCP Snooping Monitoring

1.4 Configuring Basic DHCP Snooping Functions

1.4.1 Overview

This section describes how to enable basic DHCP Snooping functions to filter out invalid DHCP packets and control the transmission scope of DHCP packets.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping globally.

ip dhcp snooping

DHCP Snooping is disabled globally by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure an interface as a DHCP Snooping trusted port.

ip dhcp snooping trust

All interfaces are DHCP Snooping untrusted ports by default.

1.5 Disabling DHCP Snooping on a VLAN

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable DHCP Snooping on a VLAN.

no ip dhcp snooping vlan { *vlan-range* | { *vlan-min* [*vlan-max*] } }

After DHCP Snooping is enabled globally, it takes effect to all VLANs by default.

1.6 Enabling Source MAC Address Verification

1.6.1 Overview

After source MAC address verification is enabled, the MAC addresses in link layer headers and the **CLIENT MAC** fields in DHCP request packets from untrusted ports are checked for consistence. If the verification fails, packets are discarded.

1.6.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable source MAC address verification.

ip dhcp snooping verify mac-address

Source MAC address verification is disabled by default.

1.7 Writing Dynamic User Information in the DHCP Snooping Binding Database to the Flash Memory in Real Time

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Write dynamic user information in the DHCP Snooping binding database to a flash memory in real time.

ip dhcp snooping database write-to-flash

1.8 Writing Dynamic User Information in the DHCP Snooping Binding Database to a Flash Memory at a Scheduled Time

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Write dynamic user information in the DHCP Snooping binding database to a flash memory at a scheduled time.

ip dhcp snooping database write-delay *time*

The function of writing all dynamic user information in the DHCP Snooping binding database to a flash memory at a scheduled time is not configured by default.

1.9 Enabling DHCP Snooping to Support BOOTP Binding

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping to support Bootstrap Protocol (BOOTP) binding.

ip dhcp snooping bootp-bind

DHCP Snooping does not support BOOTP binding by default.

1.10 Enabling DHCP Snooping to Support Relay Request Packet Processing

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping to support relay request packet processing.

ip dhcp snooping check-giaddr

DHCP Snooping does not support relay request packet processing by default.

After this function is enabled, services (IP Source Guard and Dot1x authentication) using DHCP Snooping binding entries generated based on relay requests cannot be deployed. Otherwise, users fail to access the Internet.

After this function is enabled, the **ip dhcp snooping verify mac-address** command cannot be configured. Otherwise, DHCP request packets of the relay are discarded, and users fail to obtain addresses.

1.11 Enabling DHCP Snooping to Support Binding Entry Migration

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping to support binding entry migration.

ip dhcp snooping station-move permit

DHCP Snooping does not support binding entry migration by default.

1.12 Enabling DHCP Snooping to Fast Age Client Migration Entries

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping to fast age client migration entries.

ip dhcp snooping station-move aging

Fast aging of client migration entries is enabled for DHCP Snooping by default.

1.13 Configuring an Interface in the Suppression State

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an interface in the suppression state so as to discard all DHCP packets sent to the interface.

ip dhcp snooping suppression

No interface is configured in the suppression state by default.

1.14 Configuring the Maximum Number of Users Bound to a VLAN

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum number of users bound to a VLAN.

ip dhcp snooping vlan *vlan-range* **max-user** *user-number*

The maximum number of users bound to a VLAN is not configured by default.

1.15 Configuring Option 82

1.15.1 Overview

Option 82 includes **Circuit ID** (sub-option 1) and **Remote ID** (sub-option 2). **Circuit ID** identifies the VLAN ID and interface information of a client. **Remote ID** identifies the access device of a client, which is the MAC address of the device generally.

A DHCP server assigns IP addresses based on Option 82 carried in DHCP request packets. Option 82 is transparent to clients.

1.15.2 Restrictions and Guidelines

Option 82 and DHCP Relay are mutually exclusive.

1.15.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Add Option 82 to DHCP request packets.

ip dhcp snooping information option [**standard-format** | **user-defined**]

Option 82 is not added to DHCP request packets by default.

(4) (Optional) Set **Remote ID** to a user-defined string or the host name.

ip dhcp snooping information option format remote-id { **string** *ascii-string* | **hostname** }

Remote ID in Option 82 is not set to a user-defined string or host name by default.

(5) Enter the interface configuration mode.

interface *interface-type interface-number*

(6) (Optional) Configure the VLAN in **Circuit ID** as the specified VLAN.

ip dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

When Option 82 is in extended mode, the VLAN in **Circuit ID** is not configured as the specified VLAN by default.

(7) (Optional) Set **the Circuit ID** to user-defined content.

ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id string** *ascii-string*

When Option 82 is in extended mode, **Circuit ID** is not set to user-defined content for forwarding by default.

1.16 Enabling DHCP Snooping Monitoring

1.16.1 Overview

After the DHCP Snooping monitoring function is enabled, DHCP Snooping only copies DHCP packets and generates binding entries based on the interaction status, but does not check the validity of the packets.

1.16.2 Restrictions and Guidelines

The DHCP Snooping monitoring and DHCP Snooping functions are mutually exclusive.

1.16.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping monitoring globally.

ip dhcp snooping monitor

DHCP Snooping monitoring is disabled globally by default.

1.17 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect,

the **clear** commands used for clearing information,

and the **debug** commands used for outputting debugging information.

Caution

- Running the **clear** commands may lose vital information and thus interrupt services.
- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
show ip dhcp snooping	Displays DHCP Snooping configurations.
show ip dhcp snooping binding	Displays user information in the DHCP Snooping database.
clear ip dhcp snooping binding [*ip-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Clears all dynamic users in the DHCP Snooping database.

Command	Purpose
debug snooping ipv4 event	Debugs the DHCP Snooping function based on the MAC address.
debug snooping ipv4 mac-address *H.H.H*	Debugs all DHCP Snooping functions.

1.18 Configuration Examples

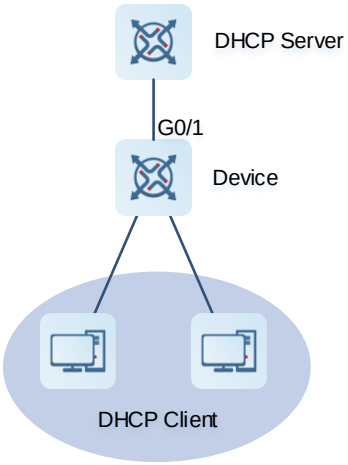
1.18.1 Configuring DHCP Snooping

1. Requirements

DHCP clients can obtain IP addresses from legitimate DHCP servers dynamically.

2. Topology

Figure 1-5 DHCP Snooping Basic Functions



3. Notes

- Enable DHCP Snooping on Device (an access device).
- Configure the uplink interface GigabitEthernet 0/1 as a trusted port.

4. Procedure

Configure Device (an access device).

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping
Device(config)# interface gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ip dhcp snooping trust
```

5. Verification

Display DHCP Snooping configurations on Device and check whether the trusted port is correct.

```
Device# show ip dhcp snooping
Switch DHCP snooping status                 :   ENABLE
DHCP snooping verify hardware address status   :   DISABLE
DHCP snooping database write-delay time       :   0 seconds
DHCP snooping option 82 status              :   DISABLE
DHCP snooping Support bootp bind status       :   DISABLE
Interface                  Trusted      Rate limit (pps)
------------------------      -------      ----------------
GigabitEthernet 0/1          YES         unlimited
```

Display entries generated by Device.

```
Device# show ip dhcp snooping binding
Total number of bindings: 1
NO.   MACADDRESS        IPADDRESS      LEASE(SEC)   TYPE         VLAN  INTERFACE
1    0013.2049.9014    172.16.1.2     86207       DHCP-Snooping 1
GigabitEthernet 0/1
```

6. Configuration Files

Device configuration file

```
hostname Device
!
ip dhcp snooping
!
interface GigabitEthernet 0/1
 ip dhcp snooping trust
!
end
```

1.19 Common Misconfigurations

- The uplink interface is not configured as a DHCP Snooping trusted port.
- Another access security option is configured for the uplink interface. As a result, the uplink interface fails to be configured as a DHCP Snooping trusted port.

Contents

1 Configuring DNS 1
1.1 Overview 1
1.2 Principles 1
1.2.1 Static Domain Name Resolution 1
1.2.2 Dynamic Domain Name Resolution 1
1.2.3 DNS Proxy 2
1.2.4 Protocols and Standards 2
1.3 Configuration Task Summary 2
1.4 Configuring Static Domain Name Resolution 3
1.5 Configuring Dynamic Domain Name Resolution 3
1.5.1 Prerequisites 3
1.5.2 Procedure 3
1.6 Configuring the Source Interface for Dynamic Domain Name Resolution 4
1.6.1 Overview 4
1.6.2 Restrictions and Guidelines 4
1.6.3 Procedure 4
1.7 Configuring DNS Proxy 5
1.7.1 Prerequisites 5
1.7.2 Procedure 5
1.8 Monitoring 6
1.9 Configuration Examples 7
1.9.1 Configuring Static Domain Name Resolution 7

1.9.2 Configuring Dynamic Domain Name Resolution 8

1.9.3 Configuring DNS Proxy 9

1 Configuring DNS

1.1 Overview

Domain Name System (DNS) is important and commonly used in a Transmission Control Protocol/Internet Protocol (TCP/IP) network environment. The main function of DNS is to convert a domain name that is easy to remember into an IP address that is hard to remember. The process of obtaining an IP address mapped to a host name is called domain name resolution (or host name resolution).

A domain name can be resolved firstly through static domain name resolution. If this fails, dynamic domain name resolution can be used instead. You can put the commonly used domain names into the static domain name resolution table, which can greatly improve the efficiency of domain name resolution.

Both the TCP and User Datagram Protocol (UDP) port IDs of DNS are 53, and generally a UDP port is used.

1.2 Principles

1.2.1 Static Domain Name Resolution

Static domain name resolution means that a user presets the mappings between domain names and IP addresses on a device. When you perform domain name operations by using application programs (such as ping and telnet), the system can find the required IP address with no need to connect to the DNS server on the network.

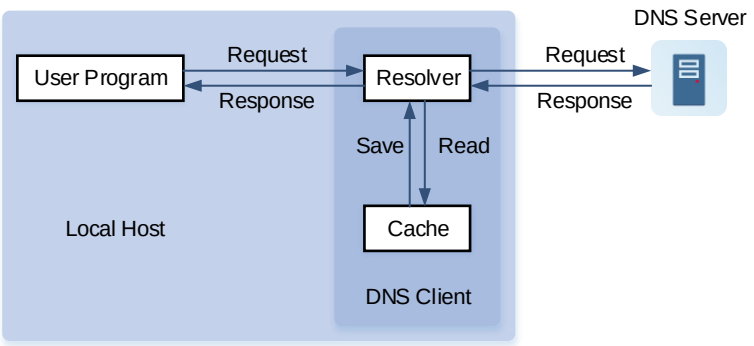
When the application programs access a small number of relatively fixed hosts, the domain name-IP mappings can be configured in advance in the form of static domain name entries. Then, no search request needs to be sent to the DNS server, improving the resolution efficiency.

1.2.2 Dynamic Domain Name Resolution

1. System Structure

Dynamic domain name resolution means that when a user performs domain name operations by using some application programs, the DNS resolver of the system queries an external DNS server for the IP addresses mapped to the domain names.

Figure 1-1 Structure of Dynamic Domain Name Resolution



As shown in Figure 1-1, a resolver is integrated with a cache to form a DNS client, which accepts DNS requests from user programs and makes responses accordingly. In general, user programs (such as ping and traceroute), a cache, and a resolver are on the same host, but a DNS server is on a different host.

2. Resolution Process

The process of dynamic domain name resolution is as follows:

(1) A user application program requests the IP address mapped to a domain name from the DNS resolver of the system.

(2) The DNS resolver queries the dynamic cache at first. If the domain name in the dynamic cache does not expire, the DNS resolver returns the domain name to the application program.

(3) If all domain names expire, the DNS resolver initiates a request for domain name-IP address conversion to the external DNS server.

(4) After receiving a response from the DNS server, the DNS resolver caches and transfers the response to the application program.

3. Cache Function

The dynamic domain name resolution supports the cache function. The cache stores the domain name-IP mappings successfully and dynamically resolved each time. When the same domain name is queried next time, the mapping can be read from the cache, with no need to send a request to the DNS server every time, thereby improving the resolution efficiency.

1.2.3 DNS Proxy

DNS proxy is generally deployed on the front-end egress gateway between a DNS server and a PC, and acts as a proxy of the DNS server to process users' DNS domain name resolution requests. When processing a request packet from the DNS client, the DNS proxy searches for the domain name-IP mapping locally first. If the required domain name-IP mapping is found, the DNS proxy directly returns it to the client. If the required domain name-IP mapping is not found, the DNS resolver searches an external DNS server for the IP address mapped to the domain name and returns a reply packet to the client.

1.2.4 Protocols and Standards

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

1.3 Configuration Task Summary

All the following configuration tasks are optional and may be selected as needed.

- Configuring Static Domain Name Resolution
- Configuring Dynamic Domain Name Resolution
- Configuring the Source Interface for Dynamic Domain Name Resolution
- Configuring DNS Proxy

1.4 Configuring Static Domain Name Resolution

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the IP address mapped to a domain name.

(IPv4 network)

ip host [**oob**] *host-name* [*telnet-port*] *ip-address* [**via** *mgmt-name*]

ip host [**vrf** *vrf-name*] *host-name* [*telnet-port*] *ip-address*(IPv6 network)

Configure the IP**v**6 address mapped to a domain name.

ipv6 host [**oob**] *host-name* [*telnet-port*] *ipv6-address* [**via** *mgmt-name*]

ipv6 host [**vrf** *vrf-name*] *host-name* [*telnet-port*] *ipv6-address*

1.5 Configuring Dynamic Domain Name Resolution

1.5.1 Prerequisites

The IP address of a DNS server has been obtained.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a DNS server.

(IPv4 network)

ip name-server [**oob**] { *ipv4-address&<1-6>* } [**via** *mgmt-name*]

No IPv4 address is configured for a DNS server by default.

(IPv6 network)

ip name-server [**oob**] { *ipv6-address&<1-6>* } [**via** *mgmt-name*]

No IPv6 address is configured for a DNS server by default.

(IPv4 network)

ip name-server [**vrf** *vrf-name*] { *ipv4-address&*<1-6> }

No IPv4 address is configured for a DNS server by default.

(IPv6 network)

ip name-server [**vrf** *vrf-name*] { *ipv6-address&*<1-6> }

No IPv6 address is configured for a DNS server by default.

1.6 Configuring the Source Interface for Dynamic Domain Name Resolution

1.6.1 Overview

If a source interface is specified in the command, when an IPv4 DNS query packet is sent, the primary IPv4 address of the source interface is used as the source address of the DNS query packet. When an IPv6 DNS query packet is sent, the first effective IPv6 address of the source interface is used as the source address of the DNS query packet.

1.6.2 Restrictions and Guidelines

If no address is configured for a source interface, a DNS query packet fails to be sent. If an IPv4 source address is specified in the command, when an IPv4 DNS query packet is sent, the configured IPv4 address serves as the source address of the IPv4 DNS query packet, and the sending of an IPv6 DNS query packet will fail. If an IPv6 source address is specified in the command, when an IPv6 DNS query packet is sent, the configured IPv6 address serves as the source address of the IPv6 DNS query packet, and the sending of an IPv4 DNS query packet will fail.

Caution

An effective IPv6 address is a unicast address, but it cannot be a local link address or a loopback address.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the domain name resolution using a specified source interface or address. The configuration steps below are mutually exclusive. Please configure only one task.

- Configure the domain name resolution using a specified source interface.

  ip domain-lookup [**oob** [**via** *mgmt-name*] | [**vrf** *vrf-name*] [**source** *interface-type interface-number*]]

- Configure the domain name resolution using a specified source IP address.

  (IPv4 network)

  ip domain-lookup [**oob** [**via** *mgmt-name*] | [**vrf** *vrf-name*] [**source ip** *ipv4-address*]]

  (IPv6 network)

  ip domain-lookup [**oob** [**via** *mgmt-name*] | [**vrf** *vrf-name*] [**source ipv6** *ipv6-address*]]

By default, no source interface is specified, and the source IP address of a DNS query packet is decided through the routing process.

1.7 Configuring DNS Proxy

1.7.1 Prerequisites

The IP address of a DNS server has been obtained.

1.7.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the DNS proxy function.

ip dns proxy enable

DNS proxy is disabled by default.

(4) (Optional) Configure the IP address mapped to a domain name.

(IPv4 network)

ip dns proxy host *host-name ipv4-address*

No static mapping between a host name and an IPv4 address is configured by default.

(IPv6 network)

ip dns proxy host *host-name ipv6-address*

No static mapping between a host name and an IPv6 address is configured by default.

(5) Configure a DNS server.

(IPv4 network)

ip dns proxy nameserver *ipv4-address*

No IPv4 address is configured for a DNS server by default.

Each time this command is run, the device will add one DNS server. The system supports up to six servers. When a domain name cannot be obtained from the first server, the device tries to send a DNS request to subsequent servers until it receives a correct reply.

(IPv6 network)

ip dns proxy nameserver *ipv6-address*

No IPv6 address is configured for a DNS server by default.

Each time this command is run, the device will add one DNS server. The system supports up to six servers. When a domain name cannot be obtained from the first server, the device tries to send a DNS request to subsequent servers until it receives a correct reply.

(6) (Optional) Enable the function of caching dynamic entries on the DNS proxy.

ip dns proxy cache

The function of caching dynamic entries is enabled on the DNS proxy by default.

(7) (Optional) Configure the time to live (TTL) of a reply packet.

ip dns proxy ttl *ttl*

The default TTL of the reply packet in response to a static entry is 3,600 seconds.

(8) (Optional) Configure the range of a source port used for query in upper-level DNS servers.

ip dns proxy port-range *port-min port-max*

The default port range is from 55000 to 58000.

This command can be used to adjust the range of a port used for query in the upper-level DNS servers. If the port range is too small, the concurrent processing performance of the device is affected. On the contrary, if the port range is too large, excessive flow table entry resources will be occupied and the egress device needs to adjust the flow table restriction synchronously.

1.8 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** command to clear information.

Caution

Running the **clear** command may lose vital information and thus interrupt services.

Table 1-1 DNS Monitoring

Command	Purpose
clear host [*host-name*]	Clears the dynamic host name cache table.
show hosts [**vrf** *vrf-name* | **oob** [**via** *mgmt-name*]] [*host-name*]	Displays DNS parameters.
debug ip dns	Debugs the DNS function.
clear dns proxy host [*host-name*]	Clears the dynamic host name cache table on the DNS proxy.
show dns proxy hosts	Displays DNS parameters on the DNS proxy.
show dns proxy statistics	Displays DNS proxy packet statistics.
debug dns-proxy	Debugs the DNS proxy.

1.9 Configuration Examples

1.9.1 Configuring Static Domain Name Resolution

1. Requirements

As shown in Figure 1-2, device A needs to access the server through the domain name www.test.com. In this case, static domain name resolution can be used to implement the access to the server whose IP address is 192.168.10.2 through the host name "www.test.com".

2. Topology

Figure 1-2 Topology of Static Domain Name Resolution

3. Notes

Manually create the mapping between www.test.com and IP address 192.168.10.2 in the static resolution table of device A.

4. Procedure

(1) Configure device A.

Configure an IP address for port GigabitEthernet 0/1.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-GigabitEthernet 0/1)# ip address 192.168.10.1 24
DeviceA(config)# exit
```

Configure the mapping between www.test.com and IP address 192.168.10.2.

```
DeviceA(config)# ip host www.test.com 192.168.10.2
```

(2) Configure the server.

Set the IP address of the server to 192.168.10.2.

5. Verification

Run the **show hosts** command to check whether the static domain name entry is configured.

```
DeviceA# show hosts
Name servers are:

Host                  type    Address         TTL(sec)
www.test.com           static   192.168.10.1       ---
```

Run the **ping** www.test.com command on device A. The IP address mapped to www.test.com is resolved as 192.168.10.2.

```
DeviceA# ping www.test.com

Translating "www.test.com"...[OK]
Sending 5, 100-byte ICMP Echoes to 192.168.10.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 ip address 192.168.10.1 24
!
 ip host www.test.com 192.168.10.2
!
```

1.9.2 Configuring Dynamic Domain Name Resolution

1. Requirements

As shown in Figure 1-3, device A is a DNS client, which can resolve domain names through the DNS server on the network.

2. Topology

Figure 1-3 Topology of Dynamic Domain Name Resolution

3. Notes

On device A, set the IP address of a DNS server to 192.168.10.2.

4. Procedure

(1) Configure device A.

Configure an IP address for port GigabitEthernet 0/1.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-GigabitEthernet 0/1)# ip address 192.168.10.1 24
DeviceA(config)# exit
```

Configure the IP address of the DNS server.

```
DeviceA(config)# ip name-server 192.168.10.2
DeviceA(config)# exit
```

(2) Configure the DNS server.

The way to configure a DNS server varies with the operating system. For details, see the configuration instructions from system vendors.

5. Verification

Run the **show hosts** command to display the configured DNS server.

```
DeviceA(config)# show hosts
Name servers are:
192.168.10.2 static

Host        type    Address                              TTL(sec)
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
 interface gigabitEthernet 0/1
 ip address 192.168.10.1 24
!
 ip name-server 192.168.10.2
!
```

1.9.3 Configuring DNS Proxy

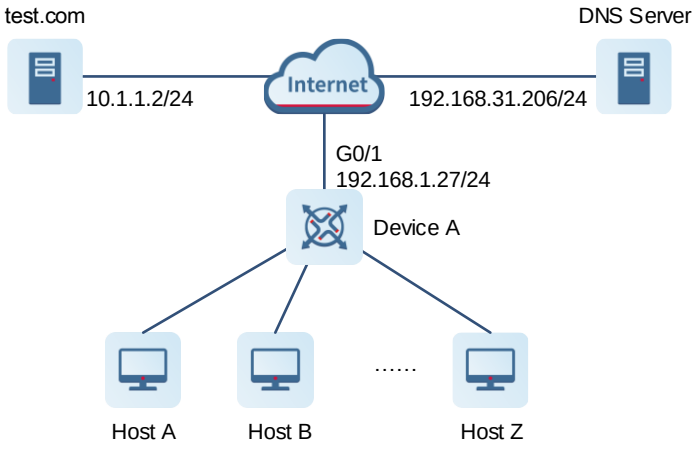
1. Requirements

As shown in Figure 1-4, a DNS server is deployed on the network to provide the domain name service for external devices. test.com is deployed on the network to provide services for external devices over test.com.

There are several hosts A-Z in the local area network (LAN). If the IP address of the DNS server is specified on each host, the network administrator needs to change the configuration of all the hosts one by one when the IP address of the DNS server changes. The workload is very heavy. Device A in the LAN needs to configured as a DNS proxy, the IP address of the DNS server specified on the DNS proxy is the real address of the DNS server. In this way, when the IP address of the DNS server changes, only the configuration on the DNS proxy needs to be changed, which can greatly reduce the workload.

2. Topology

Figure 1-4 Topology of DNS Proxy



3. Notes

- On device A, enable the DNS proxy function.
- On device A, set the IP address mapped to test.com to 10.1.1.2/24.
- On device A, set the IP address of the DNS server to 192.168.31.206/24.

4. Procedure

(1) Configure device A.

Configure an IP address for port GigabitEthernet 0/1.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-GigabitEthernet 0/1)# ip address 192.168.1.27 24
DeviceA(config-GigabitEthernet 0/1)# exit
```

Configure the DNS proxy function.

```
DeviceA(config)# ip dns proxy enable
DeviceA(config)# ip dns proxy host test.com 10.1.1.2
DeviceA(config)# ip dns proxy nameserver 192.168.31.206
DeviceA(config)# exit
```

(2) Configure the DNS server.

The way to configure a DNS server varies with the operating system. For details, see the configuration instructions from system vendors.

5. Verification

Run the **show dns proxy hosts** command to check whether the DNS proxy is configured.

```
DeviceA(config)# show dns proxy hosts
proxy state: enable
Name servers are:
```

```
192.168.31.206

static host    max: 1024
static host   count: 1
cache domain    max: 5120
cache domain  count: 0
Host                     type          TTL(sec)       Address
host.com                  static         ---           192.168.31.206
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
interface gigabitethernet 0/1
ip address 192.168.1.27 24
!
ip dns proxy enable
ip dns proxy host test.com 10.1.1.2
ip dns proxy nameserver 192.168.31.206
!
```

Contents

1 Configuring IPv6 Basics 1
1.1 Overview 1
1.2 Advantages 1
1.3 Principles 2
1.3.1 IPv6 Basics 2
1.3.2 ICMPv6 Protocol 12
1.3.3 IPv6 PMTUD 13
1.3.4 IPv6 Neighbor Discovery Protocol 14
1.3.5 Protocols and Standards 17
1.4 Configuring IPv6 Basic Information 17
1.4.1 Overview 17
1.4.2 Configuration Task Summary 17
1.4.3 Configuring an IPv6 Address 18
1.4.4 Configuring the IPv6 MTU for an Interface 19
1.4.5 Configuring IPv6 Source Routing 19
1.4.6 Configuring the IPv6 Hop Limit 20
1.4.7 Configuring the Default Gateway for a Management Interface 20
1.4.8 Configuring the Specified Source Address for Sending ICMPv6 Packets 21
1.4.9 Configuring the Transmission Rate of ICMPv6 Error Messages 21
1.5 Configuring IPv6 NDP 22
1.5.1 Overview 22
1.5.2 Configuration Task Summary 22

1.5.3 Configuring a Static Neighbor Entry 23

1.5.4 Configuring ND Entry Management 23

1.5.5 Configuring Address Resolution 25

1.5.6 Configuring NUD 26

1.5.7 Configuring DAD 27

1.5.8 Configuring Redirection 27

1.5.9 Configuring Parameters Related to RA Packets 28

1.5.10 Configuring ND Logging 29

1.5.11 Configuring the Interval for ND Packet Rate Statistics Collection 30

1.5.12 Configuring Local ND Proxy 30

1.5.13 Configuring the ND Protocol to Allocate Different Prefixes to Different Users 31

1.5.14 Restraining an Interface from Sending NS Packets to Authenticated VLANs 31

1.6 Monitoring 32

1.7 Configuration Examples 33

1.7.1 Manually Configuring IPv6 Addresses 33

1.7.2 Enabling Stateless IPv6 Address Auto-configuration 35

1 Configuring IPv6 Basics

1.1 Overview

As the Internet develops rapidly and IPv4 address space is becoming exhausted, IPv4 limitations become more and more obvious. At present, many researches and practices on Internet Protocol Next Generation (IPng) have been conducted. The IPng working group of the Internet Engineering Task Force (IETF) has formulated an IPng protocol named IP Version 6 (IPv6).

1.2 Advantages

- Larger address space

Compared with 32-bit IPv4 addresses, the length of an IPv6 address is extended to 128 bits. Therefore, the address space has approximately 2^{128} addresses. IPv6 supports a hierarchical address allocation mode from the Internet core network to intranet subnet.

- Simplified packet header format

Since the design principle of the IPv6 packet header is to minimize the cost of the packet header, some non-key fields and optional fields are removed from the packet header to the extended packet header. Therefore, although the length of an IPv6 address is four times that of an IPv4 address, the IPv6 packet header is only twice the IPv4 packet header in length. Without the checksum field in the IPv6 packet header, IPv6 devices do not need to process fragments during forwarding. Therefore, the packet can be more efficiently forwarded.

- Efficient hierarchical addressing and routing structure

IPv6 uses a convergence mechanism and defines a flexible hierarchical addressing and routing structure. Multiple networks at the same layer are represented with a uniform network prefix on the upstream device, greatly reducing routing entries maintained by the device and routing and storage costs of the device.

- Easy management: plug and play (PnP)

IPv6 provides automatic discovery and auto-configuration functions to simplify management and maintenance of network nodes. For example, neighbor discovery (ND), maximum transmission unit (MTU) discovery, router advertisement (RA), router solicitation (RS), and auto-configuration technologies provide related services for PnP.

IPv6 supports stateful and stateless address configuration modes. In IPv4, Dynamic Host Configuration Protocol (DHCP) realizes auto-configuration of the host IP addresses and related parameters. IPv6 inherits this auto-configuration service from IPv4, which is called stateful auto-configuration. For details, see "Configuring DHCPv6". Besides, IPv6 also offers the stateless auto-configuration service. During stateless auto-configuration, a host automatically obtains the link-local address, address prefix of the local device, and other parameter configurations.

- Security

Internet Protocol Security (IPSec) is an optional extension protocol of IPv4 but a part of IPv6 to ensure security of IPv6. At present, IPv6 provides two mechanisms: authentication header (AH) and encapsulated security payload (ESP). AH ensures data integrity and authenticates IP packet sources to ensure that the packets are

from the nodes identified by the source addresses. ESP provides data encryption to realize end-to-end encryption.

- Better QoS support

A new field in the IPv6 packet header defines how to identify and process data streams. The **Flow Label** field in the IPv6 packet header is used to authenticate a data stream, and users can propose requirements on the communication quality by using this field. A device can identify all packets belonging to a specific data stream based on this field and process these packets according to user requirements.

- New protocol for neighboring node interaction

IPv6 Neighbor Discovery Protocol (NDP) uses a series of Internet Control Message Protocol Version 6 (ICMPv6) packets to implement interactive management of adjacent nodes (nodes on the same link). IPv6 uses NDP packets and efficient multicast/unicast ND packets to replace the broadcast-based Address Resolution Protocol (ARP) and Internet Control Message Protocol Version 4 (ICMPv4) router discovery packets.

- Extensibility

IPv6 features strong extensibility, allowing users to add new features to the extension packet headers following the IPv6 packet header. The IPv4 packet header supports at most 40 bytes of options. By contrast, the length of an IPv6 extension packet header is subject to only the maximum number of bytes in the packet.

1.3 Principles

1.3.1 IPv6 Basics

1. IPv6 Address Format

An IPv6 address is represented in the X:X:X:X:X:X:X format. A 128-bit IPv6 address is separated into eight groups by colons (:), and the 16 bits in each group are represented by four hexadecimal characters (0-9, A-F). Each "X" represents a group of four hexadecimal values. The following are three valid IPv6 addresses:

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800:0:0:0:0:0:0:1

1080:0:0:0:8:800:200C:417A

To simplify the writing of IPv6 addresses, the number "0" in an IPv6 address can be abbreviated as follows:

- Each integer in the address must be represented, except the leading zeros in each integer. For example, 2001:00CD:0034:0078:000A:000B:1200:2100 can be abbreviated as 2001:CD:34:78:A:B:1200:2100.
- If an IPv6 address contains a string of zeros, double colons (::) can be used to represent these zeros. For example, 800:0:0:0:0:0:0:1 can be represented as 800::1. The double colons indicate that this address can be extended to a complete 128-bit address. In this approach, only when the 16-bit integers are all zeros, can they be replaced with double colons. Double colons can exist only once in an IPv6 address.

In an IPv4/IPv6 hybrid environment, in an IPv6 address, the least significant 32 bits can be used to represent an IPv4 address. This IPv6 address can be represented in a hybrid manner, that is, X:X:X:X:X:X:d.d.d.d, "X" is a hexadecimal integer and "d" is an 8-bit decimal integer. For example, 0:0:0:0:0:0:192.168.20.1 is a valid IPv6 address. It can be abbreviated to ::192.168.20.1. One typical application of this hybrid representation is to map an IPv4 address to an IPv6 address, for example, IPv4 address 1.1.1.1 is mapped to an IPv6 address ::FFFF:1.1.1.1.

2. IPv6 Address Structure

An IP address consists of two parts:

- Network prefix: n bits, similar to the network ID in an IPv4 address.
- Interface ID: (128 – n) bits, similar to the host ID in an IPv4 address.

Therefore, the length of the network prefix can be expressed using an additional value according to the classless inter-domain routing (CIDR), and this value is separated from an IPv6 address by a slash (/), for example, 12AB::CD30:0:0:0:0/60, the prefix length used for routing in the address is 60 bits.

3. IPv6 Address Type

RFC 4291 defines three types of IPv6 addresses:

- Unicast address: ID of a single interface. Packets destined to a unicast address are sent to the interface identified by this address.
- Multicast address: ID of an interface group (the interfaces generally belong to different nodes). Packets destined to a multicast address are sent to all interfaces included in this address.
- Anycast address: ID of an interface group. Packets destined to an anycast address are sent to one of the interfaces included in this address (the nearest interface according to the routing protocol).

Note

IPv6 does not define broadcast addresses.

4. Unicast Addresses

Unicast addresses are classified into five types: unspecified address, loopback address, link-local addresses, site-local addresses, and global unicast addresses. Currently site-local addresses have been abolished.

- Unspecified address

  The unspecified address is 0:0:0:0:0:0:0:0, which is usually abbreviated to ::. It has two general purposes:

  - If a host has no unicast address when started, it uses the unspecified address as the source address to send an RS packet to obtain prefix information from the gateway and thereby generate a unicast address.
  - When an IPv6 address is configured for a host, the device detects whether the address conflicts with addresses of other hosts in the same network segment and uses the unspecified address as the source address to send a neighbor solicitation (NS) packet (similar to a gratuitous ARP packet).

- Loopback address

  The loopback address is 0:0:0:0:0:0:0:1, which is usually abbreviated to ::1. Similar to IPv4 address 127.0.0.1, the loopback address is generally used by a node to send packets to itself.

- Link-local address

  The format of a link-local address is as follows:

Figure 1-1 Link-Local Address

10 bits	54 bits	64 bits
1111 1110 10	0	Interface ID

A link-local address is used to number hosts on a single network link. The address identified by the first 10 bits in the prefix is the link-local address. A device will not forward packets in which the source or destination address contains the link-local address. The middle 54 bits of this address is 0, and the last 64 bits represent the interface ID. The address part in the middle allows a single network to connect up to 2^{64} – 1 hosts.

IPv6 link-local addresses can be generated automatically by a device or specified manually.

- Site-local address

  The format of a site-local address is as follows:

Figure 1-2 Site-Local Address

10 bits	54 bits	64 bits
1111 1110 11	Subnet ID	Interface ID

A site-local address can be used to transmit data within a site. A device never forwards packets in which the source or destination address contains a site-local address to the Internet. A site can be assumed as an enterprise's local area network (LAN). Such addresses are similar to IPv4 private addresses such as 192.168.0.0/16. RFC 3879 has abolished site-local addresses. New addresses do not support this prefix and are all regarded as global unicast addresses. Existing addresses can continue to use this prefix.

- Global unicast address

  Except unspecified, loopback, and link-local addresses, all other unicast addresses are global unicast addresses. The format of a global unicast address is as follows:

Figure 1-3 Global Unicast Address

n bits	m bits	128-n-m bits
Global routing prefix	Subnet ID	Interface ID

Among global unicast addresses, there is a type of IPv4-embedded IPv6 addresses, including IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. They are used for interconnection between IPv4 nodes and IPv6 nodes.

  - The format of an IPv4-compatible IPv6 address is as follows:

Figure 1-4 Format of an IPv4-compatible IPv6 Address

80 bits	16 bits	32 bits
0000.....0000	0000	IPv4 address

- The format of an IPv4-mapped IPv6 address is as follows:

Figure 1-5 Format of an IPv4-mapped IPv6 Address

80 bits	16 bits	32 bits
0000.....0000	FFFF	IPv4 address

IPv4-compatible IPv6 addresses are mainly used on automatic tunnels. Nodes on automatic tunnels support both IPv4 and IPv6. Using these addresses, IPv4 devices transmit IPv6 packets over tunnels. At present, IPv4-compatible IPv6 addresses have been abolished. IPv4-mapped IPv6 addresses are used by IPv6 nodes to access IPv4-only nodes. For example, if an IPv6 application on an IPv4/IPv6 host requests to resolve the name of an IPv4-only host, the name server dynamically generates an IPv4-mapped IPv6 address and returns it to the IPv6 application.

5. Multicast Addresses

One IPv6 multicast address usually identifies interfaces on a series of different nodes. After a packet is sent to a multicast address, the packet is then forwarded to the interfaces on each node identified by this multicast address.

A multicast address is prefixed with FF00::/8. The format of an IPv6 multicast address is as follows:

Figure 1-6 Multicast Address

8 bits	4 bits	4 bits	112 bits
11111111	Flag	Range	Multicast group ID

- Flag field

  The flag field consists of four bits. Currently only the fourth bit is specified. If this flag bit is 0, the address is a permanent known multicast address assigned by the Internet Assigned Numbers Authority (IANA). If this flag bit is 1, the address is a temporary multicast address used in a certain scenario. The remaining three flag bits are reserved for future use and set to 0.

- Scope field:

  The scope field consists of four bits to indicate the scope type of a multicast address. The following table lists common multicast address scope types and their corresponding values. Unlisted values indicate reserved or unspecified.

Table 1-1 Common Multicast Address Scope Types

Binary Value	Hexadecimal Value	Scope Type
0001	1	Local interface scope
0010	2	Local link scope
0011	3	Local subnet scope
0100	4	Local management scope
0101	5	Local site scope
1000	8	Organization scope
1110	E	Global scope

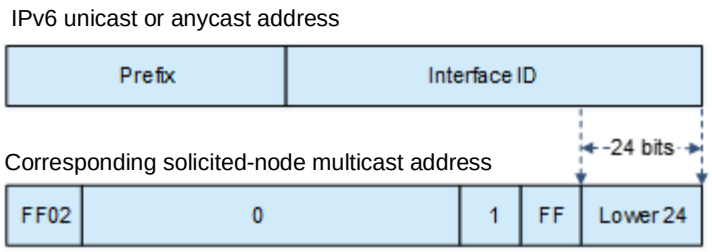
- Multicast group ID field:

  The multicast group ID field consists of 112 bits to identify a multicast group. A multicast group ID can represent different groups based on the flag and scope fields.

Multicast addresses for special purposes:

- FF01::1 represents the multicast address of all nodes in the node-local scope.
- FF02::1 represents the multicast address of all nodes in the link-local scope.
- FF01::2 represents the multicast address of all devices in the node-local scope.
- FF02::2 represents the multicast address of all devices in the link-local scope.
- Solicited-node multicast address. The address is mainly used to obtain the link layer address of a neighbor node on the same link and perform the duplicate address detection. Each unicast or anycast IPv6 address has a corresponding solicited-node address. The address is in the format of FF02:0:0:0:0:1:FFXX:XXXX, FF02:0:0:0:0:1:FF is the fixed 104 bits, and XX:XXXX is the last 24 bits of a unicast or anycast IPv6 address. Solicited-node multicast addresses are usually used in NS packets. The address format is as follows:

Figure 1-7 Format of a Solicited-Node Multicast Address



6. Anycast Addresses

Similar to a multicast address, an anycast address can also be shared by multiple nodes. The difference is that only one node using the anycast address receives data packets while all nodes using the multicast address receive data packets. Since anycast addresses are allocated from the normal IPv6 unicast address space, they use the same format as unicast addresses. Therefore, each member of an anycast address group must be configured explicitly for easier recognition.

Caution

Anycast addresses can be allocated only to devices not hosts and cannot be used as source addresses of packets.

RFC 2373 defines an anycast address called subnet-router anycast address. The following figure shows the format of a subnet-router anycast address. Such an address consists of the subnet prefix and a series of zeros (interface ID).

The subnet prefix identifies a specified link (subnet). Packets destined to the subnet-router anycast address will be forwarded to a device on this subnet. A subnet-router anycast address is usually used by the application on a node to communicate with a device on a remote subnet.

Figure 1-8 Format of a Subnet Router Anycast Address

Note

The format of an anycast address is shown in Figure 1-8, that is, n bits of subnet prefix plus (128 – n) bits of all zeros. For example, in the anycast address 1000:1::100/120, the length of the subnet prefix is 120 bits, and the host address is 8-bit all zeros. An anycast address cannot be used as the interface address of a switch.

7. IEEE EUI-64 Interface ID

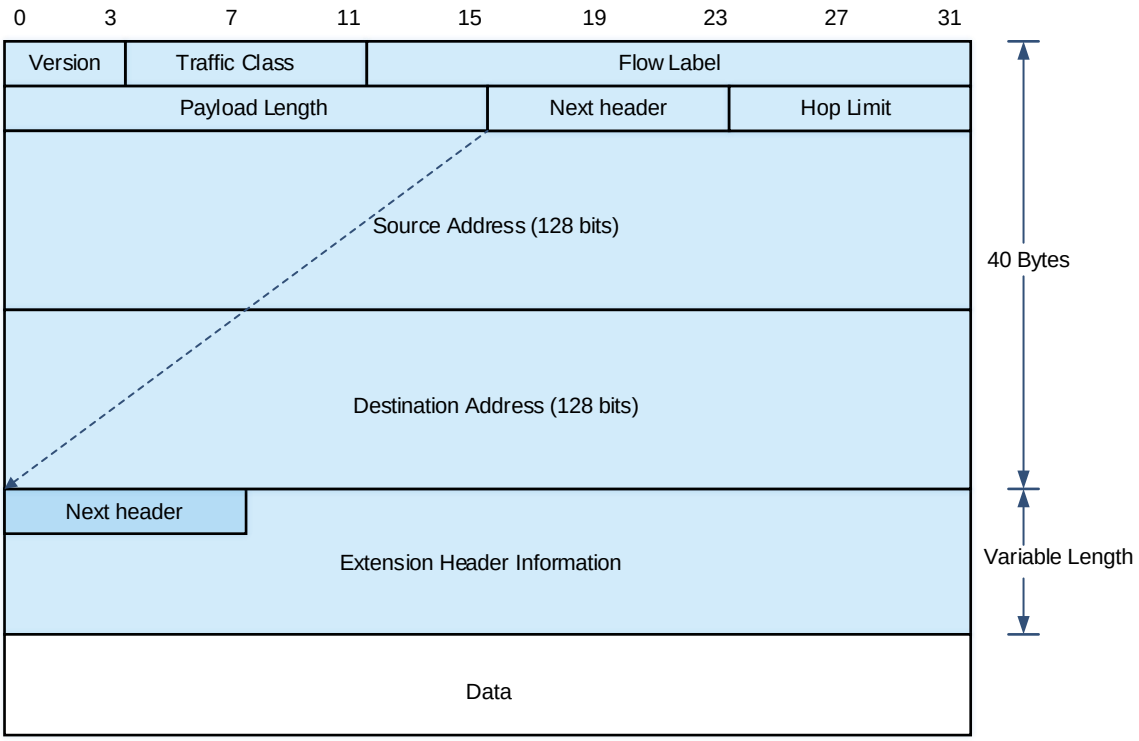
The 64-bit interface ID in an IPv6 address is used to identify a unique interface on the link. This address is a variation of a link-layer address (such as an MAC address) of an interface. This address is generated by inserting a hexadecimal number FFFE after the 24th bit of an MAC address. To make the scope of an interface ID the same as the original MAC address, the U/L bit (the 7th bit starting from the most significant bit) is negated. The resulting set of numbers is used as the interface ID in EUI-64 format.

For the loopback, VBDIF, and tunnel interfaces, the EUI-64 addresses are generated from the MAC addresses of these interfaces, with the last two bytes of the interface index filled in the middle.

8. Format of an IPv6 Packet Header

The format of an IPv6 packet header is shown in the following figure.

Figure 1-9 Format of an IPv6 Packet Header



The IPv6 packet header consists of 40 bytes, in unit of eight bytes. An IPv6 packet header has the following fields:

- Version

  This field consists of 4 bits. In an IPv6 address, this field must be 6.

- Traffic Class

  This field consists of 8 bits. This field indicates the service provided for this packet, and is similar to the type of service (ToS) field in an IPv4 address.

- Flow Label

  This field consists of 20 bits to identify packets belonging to the same service flow. One node can act as the transmission source of multiple service flows. The flow label and source node address uniquely identify one service flow.

- Payload Length

  This field consists of 16 bits, including the packet payload length and the length of IPv6 extended options (if available). That is, it includes the IPv6 packet length except the IPv6 packet header.

- Next Header

  This field indicates the protocol type in the header field following the IPv6 packet header. Similar to the protocol field in the IPv4 address header, the **Next Header** field is used to indicate whether the upper layer uses Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). It can also be used to indicate existence of an IPv6 extension header.

- Hop Limit

This field contains eight bits. Every time a device forwards a packet, the hop value is reduced by 1. If the hop value reaches 0, this packet will be discarded. It is similar to the lifetime field in the IPv4 packet header.

- Source Address

  This field consists of 128 bits and indicates the sender address in an IPv6 packet.

- Destination Address

  This field consists of 128 bits and indicates the receiver address in an IPv6 packet.

At present, IPv6 defines the following extension headers.

- Hop-By-Hop Options

  This extension header must follow the IPv6 packet header. It consists of option data to be checked on each node along the path.

- Routing Options

  This extension header indicates the nodes that a packet passes through from the source address to the destination address. It consists of the address list of the passerby nodes. The initial destination address in an IPv6 packet header is the first address among the addresses in the routing header, but not the final destination address of the packet. After the node corresponding to the destination address in an IPv6 packet header receives the packet, it processes the IPv6 packet header and routing header, and sends the packet to the second address, the third address, and so on in the list in the routing header till the packet reaches the final destination address.

- Fragment

  The source node uses this extension header to fragment the packets, of which the length exceeds the path MTU (PMTU).

- Destination Options

  This extension header replaces the option fields of IPv4. At present, the **Destination Options** field can only be filled with integral multiples of 64 bits (eight bytes) if required. This extension header can be used to carry information to be checked by the destination node.

- Upper-layer Header

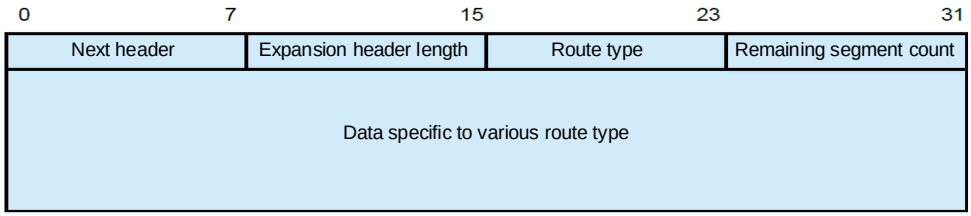
  This extension header indicates the protocol used by the upper layer for data transmission, such as TCP (6) and UDP (17).

Another two extension headers **Authentication** (AH) and **Encapsulating Security Payload** (ESP) will be described in "Configuring IPSec" in "VPN Configuration Guide".

9. IPv6 Source Routing

Similar to the IPv4 loose source routing and loose record routing options, the IPv6 routing header is used to specify the intermediate nodes that a packet passes through. It uses the following format:

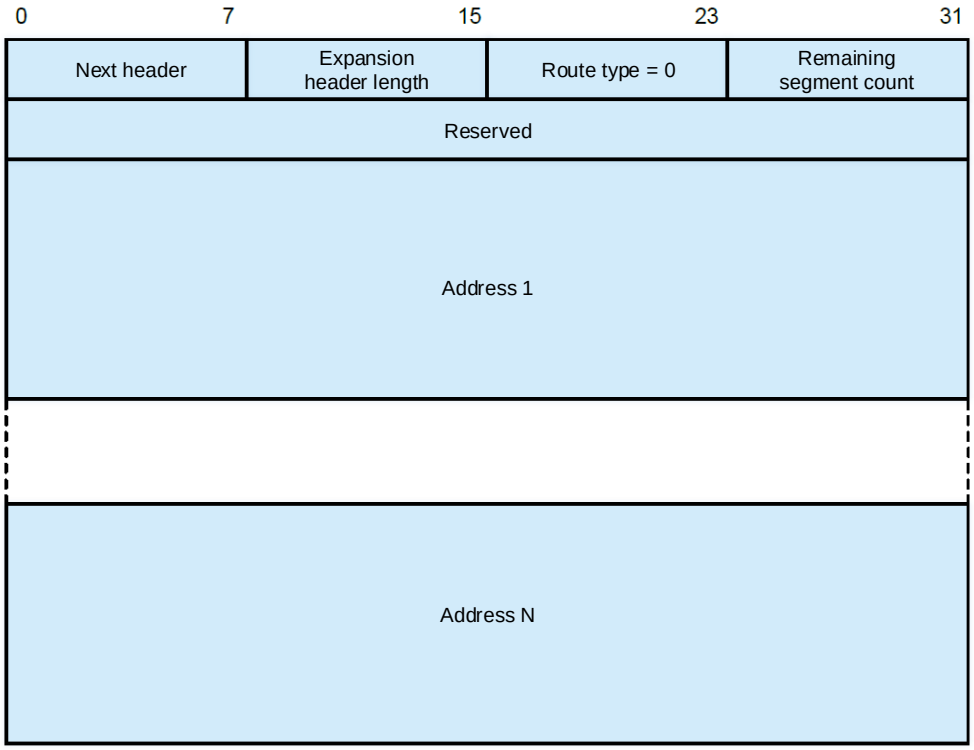
Figure 1-10 IPv6 Routing Header



The **Segments Left** field is used to indicate the number of intermediate nodes specified in the routing header that a packet passes through from the current node to the final destination address.

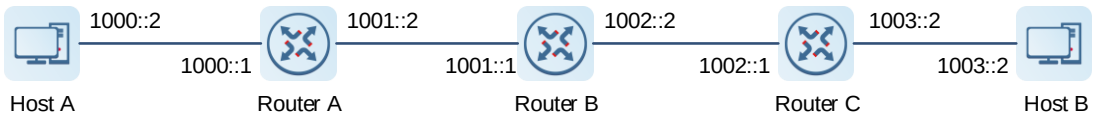
Currently, two routing types are defined: 0 and 2. The Type 2 routing header is used for mobile communication. Type 0 routing header is similar to the loose source routing option of IPv4. The format of the Type 0 routing header is as follows:

Figure 1-11 Type 0 Routing Header



The example describes the application of the Type 0 routing header.

Figure 1-12 Applications of the Type 0 Routing Header



Host A sends host B a packet, which specifies the intermediate nodes router B and router C. The following table lists the changes of fields related to the IPv6 header and routing header during the forwarding process.

Table 1-2 Changes of Fields

Transmission Node	Fields in the IPv6 Header	Fields Related to the Type 0 Routing Header
Host A	Source address = 1000::2 Destination address = 1001::1 (address of router 2)	Segments Left = 2 Address 1 = 1002::1 (address of router 3) Address 2 = 1003::2 (address of host 2)
Router A	No change	
Router B	Source address = 1000::2 Destination address = 1002::1 (address of router 3)	Segments Left = 1 Address 1 = 1001::1 (address of router 2) Address 2 = 1003::2 (address of host 2)
Router C	Source address = 1000::2 Destination address = 1003::2 (address of host 2)	Segments Left = 0 Address 1 = 1001::1 (address of router 2) Address 1 = 1002::2 (address of router 3)
Host B	No change	

The forwarding process is described as follows:

(1) Host A sends a packet in which the destination address is router B's address 1001::1, the Type 0 routing header is filled with router C's address 1002::1 and host B's address 1003::2, and the value of the **Segments Left** field is **2**.

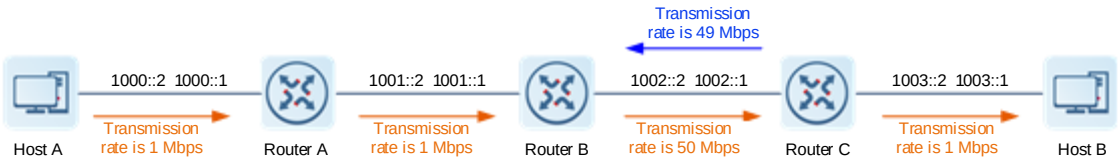
(2) Router A forwards the packet to router B.

(3) Router B interchanges the destination address in the IPv6 header with address 1 in the routing header. That is, the destination address becomes router C's address 1002::1, address 1 in the routing header becomes router B's address 1001::1, and the value of the **Segments Left** field becomes **1**. After modification, router B forwards the packet to router C.

(4) Router C interchanges the destination address in the IPv6 header with address 2 in the routing header. That is, the destination address becomes host B's address 1003::2, address 2 in the routing header becomes router C's address 1002::1, and the value of the **Segments Left** field becomes **0**. After modification, router C forwards the packet to host B.

The Type 0 routing header may be used to initiate denial of service (DoS) attacks. As shown in the following figure, host 1 sends a packet to host 2 at a rate of 1 Mbps and forges a routing header with the **Segments Left** field of 100 to cause multiple round-trips of the packet between router 2 and router 3 (50 times from router 2 to router 3 and 49 times from router 3 to router 2). At the time, the routing header generates the traffic amplification effect: 50 Mbps from router 2 to router 3 and 49 Mbps from router 3 to router 2. Due to this security problem, RFC 5095 abolished the Type 0 routing header.

Figure 1-13 Type 0 Routing Header Used to Initiate DoS Attacks



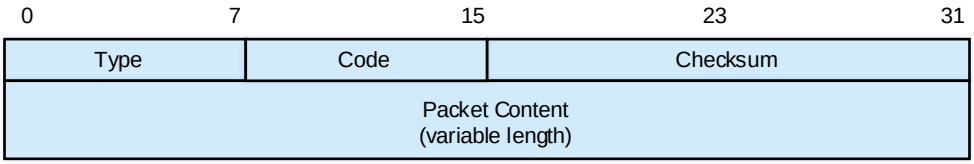
10. IPv6 Hop-limit

An IPv6 data packet passes through routers from the source address to the destination address. If a hop limit is configured, it decreases by one every time the packet passes through a router. When the hop limit decreases to 0, the router discards the packet to prevent this useless packet from being unlimitedly transmitted on the network and wasting network bandwidth. The hop limit is similar to the time to live (TTL) of IPv4.

1.3.2 ICMPv6 Protocol

1. Packet Format

Figure 1-14 ICMPv6 Packet Format



Field descriptions are as follows:

- The **Type** field indicates the type of a packet, 0 to 127 indicates error messages, and 128 to 255 indicates informational messages.
- The **Code** field indicates the subdivision type of this message type.
- The **Checksum** field indicates the checksum of ICMPv6 packets.

2. ICMPv6 Error Messages

ICMPv6 error messages are sent by a destination node or intermediate router to report the errors incurred during IPv6 data packet forwarding and transmission. There are mainly four types of error messages:

- Destination Unreachable (Type=1), indicating that packets cannot be forwarded to the destination node or the upper-layer protocol.
  - Code=0, indicating that there is no route reachable to the destination.
  - Code=1, indicating that the communication with the destination is prohibited according to the administration policy.
  - Code=2, unspecified.
  - Code=3, address unreachable.
  - Code=4, port unreachable.
- Packet Too Big (Type = 2, Code = 0), indicating that the size of a packet exceeds the link MTU of an

interface.

- Time Exceeded (Type=3)
  - Code=0, indicating that the hop limit is exceeded during transmission.
  - Code=1, fragmentation timeout.
- Parameter Problem (Type=4), indicating that an error occurs in the IPv6 header or extension header.
  - Code=0, indicating an incorrect header field.
  - Code=1, indicating that the next header cannot be identified.
  - Code=2, indicating that the IPv6 option cannot be identified.

3. ICMPv6 Informational Messages

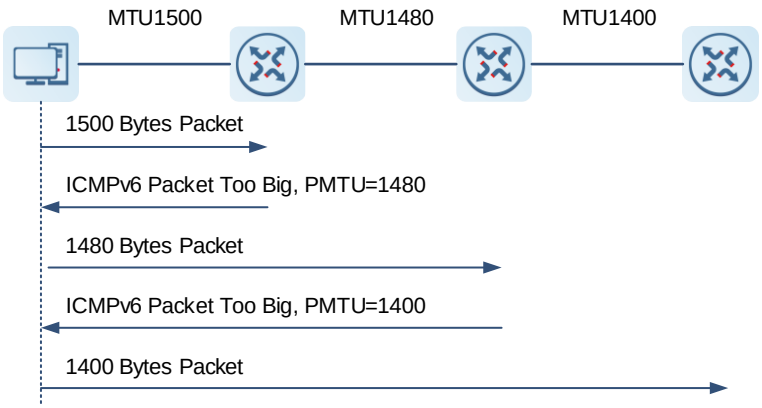
The following describes common informational messages:

- Type=128, echo request, which is sent to the destination node to trigger the destination node to immediately send back an echo reply packet.
- Type=129, echo reply, which is sent in response to an echo request.
- Type=133, router solicitation (RS) packet. After a node is started, it initiates a solicitation to the router via an RS packet to request the prefix and other configurations.
- Type=134, router advertisement (RA) packet, which is sent in response to an RS packet and advertises prefix options and certain flag bits.
- Type=135, neighbor solicitation (NS) packet, which is similar to an ARP request and used to obtain the link layer address of a neighbor, check whether the neighbor is reachable, and perform duplicate address detection.
- Type=136, neighbor advertisement (NA) packet, which is similar to an ARP reply packet.
- Type=137, Redirect packet. By sending a Redirect packet to the source host, the default gateway triggers the host to re-select a better next-hop address for delivering subsequent packets.

1.3.3 IPv6 PMTUD

Similar to IPv4 path MTU discovery (PMTUD), IPv6 PMTUD allows a host to dynamically discover the MTU size in the data path. If the length of a data packet to be sent by a host is greater than the PMTU, the host performs packet fragmentation.

Figure 1-15 IPv6 PMTUD



As shown in the preceding figure, if the length of a packet to be sent by a host is greater than the PMTU, the router discards this packet and sends an ICMPv6 Packet Too Big message containing its PMTU to the host. The host fragments the packet based on the new PMTU. In this manner, the router does not need to perform fragmentation, saving router resources and improving the IPv6 network efficiency.

1.3.4 IPv6 Neighbor Discovery Protocol

Neighbor Discovery Protocol (NDP) is a basic part of IPv6. Its main functions include router discovery, prefix discovery, parameter discovery, address auto-configuration, address resolution (like ARP), next-hop determination, neighbor unreachability detection (NUD), duplicate address detection (DAD), and redirection.

NDP defines five types of ICMP packets: RS, RA, NS, NA, and Redirect.

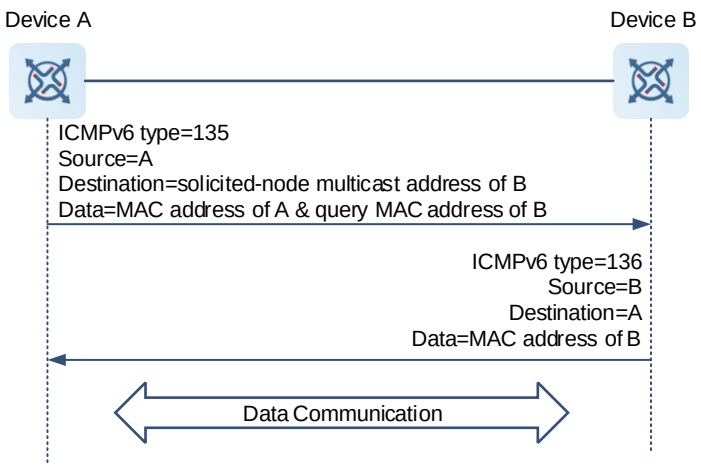
All the above ICMP packets carry one or more options. These options are optional in some cases but are significant in other cases. NDP mainly defines five options: **Source Link-Layer Address** option, Type = 1; **Target Link-Layer Address** option, Type = 2; **Prefix Information** option, Type = 3; **Redirect Header** option, Type = 4; **MTU** option, Type = 5.

Different NDP mechanisms use different ICMPv6 messages.

1. Address Resolution

When a node attempts to communicate with another, the node has to obtain the link-layer address of the peer by sending an NS packet to the peer. In this packet, the destination address is the solicited-node multicast address corresponding to the IPv6 address of the destination node. This packet also contains the link-layer address of the source node. After receiving this NS packet, the destination node replies with an NA packet, in which the destination address is the source address of the NS packet and the content is the link-layer address of the solicited node. After receiving this NA packet, the source node can communicate with the destination node.

Figure 1-16 Address Resolution



The process of address resolution is as follows:

(1) Device A sends an NS packet in multicast mode. The source address of the NS packet is the IPv6 address of the interface of device A, and the destination address is the solicited-node multicast address of device B. The packet contains the link layer address of device A, and solicits the link layer address of device B.

(2) After receiving the NS packet, device B judges whether the destination address of the packet is its own IPv6 address. If yes, device B can learn the link layer address of device A and returns an NA packet containing its link layer address in unicast mode.

(3) Device A can get the link layer address of device B from the received NA packet. The two devices can then begin to communicate with each other.

2. NUD

If the amount of time that a neighbor is considered reachable has elapsed but an IPv6 unicast packet needs to be sent to the neighbor, the device performs NUD. The NS and NA packets can be used to detect whether the neighbor node is reachable.

(1) The node sends an NS packet, in which the destination address is the IPv6 address of the neighbor node.

(2) If the acknowledgment packet is received from the neighbor node, the neighbor is considered reachable. Otherwise, the neighbor is considered unreachable.

While NUD is underway, the device can continue to forward IPv6 packets to the neighbor.

3. DAD

When obtaining an IPv6 address, a node needs to perform DAD to determine whether the IPv6 address is unique on the link. This feature is similar to the gratuitous ARP in IPv4.

The process of DAD is as follows:

(1) A node sends an NS packet. The source IPv6 address of the NS packet is the unspecified address, and the destination address is the solicited-node multicast address corresponding to the IPv6 address to be detected. The packet content is the IPv6 address to be detected.

(2) After receiving the NS packet, other neighbor nodes check whether the IPv6 address exists in their local IPv6 address collections. If yes, the neighbor node that has the IPv6 address responds with an NA packet that carries the IPv6 address to the source node.

(3) When receiving the NA packet from the neighbor, the source node considers the IPv6 address in use. On the contrary, if the source node receives no NA packet in response to the NS packet, the IPv6 address is available.

If a device detects an address conflict, this address is set in the duplicate state and the device cannot receive IPv6 packets destined to this address. Meanwhile, the device also starts a timer for this duplicate address to periodically perform DAD. If no address conflict is detected, this address can be properly used.

4. RA Packets

An RA packet usually contains the following content:

- One or more IPv6 address prefixes (used for on-link determination or stateless address auto-configuration);
- Validity period of the IPv6 address prefix;
- Host auto-configuration method (stateful or stateless);
- Default device information (whether the device acts as the default device; if yes, the duration for acting as the default device is also included);
- Other information provided for host configuration, such as hop limit, MTU and NS retransmission interval.

RA packets can also be used as replies to the RS packets sent by a host. Using RS packets, a host can obtain the auto-configured information immediately after startup rather than wait for the RA packets sent by the device.

If no unicast address is configured for a newly started host, the host uses the unspecified address (0:0:0:0:0:0:0:0) as the source address of the RS packet. Otherwise, the host uses the configured unicast address as the source address and the multicast address of all devices in the local link (FF02::2) as the destination address in the RS packet. As a reply to the RS packet, the RA packet uses the source address of the RS packet as the destination address. If the source address is the unspecified address, it uses the multicast address of all nodes in the local link (FF02::1).

In an RA packet, the following parameters can be configured in the IPv6 interface attributes:

- Ra-interval: Indicates the interval for sending the RA packets.
- Ra-lifetime: Indicates the lifetime of a router, that is, whether the device acts as the default router on the local link and the duration for acting as the default router.
- Prefix: Indicates the prefix of an IPv6 address of the local link. It is used for on-link determination or stateless address auto-configuration, including other parameter configurations related to the prefix.
- Ns-interval: Indicates the NS packet retransmission interval.
- Reachable-time: Indicates the period in which the device regards a neighbor reachable after detecting the neighbor reachability event.
- Ra-hoplimit: Indicates the hop count in an RA packet, which is used to set the hop limit for a host to send a unicast packet.
- Ra-mtu: Indicates the value of the MTU field in an RA packet.
- Managed-config-flag: Determines whether a host receiving this RA packet obtains the address through stateful auto-configuration.
- Other-config-flag: Determines whether a host receiving this RA packet uses DHCPv6 to obtain other information except the IPv6 address for auto-configuration.
- RDNSS and DNSSL options: Provide IPv6 terminals with the address of the DNS recursive query server and a search list of DNS domain names.

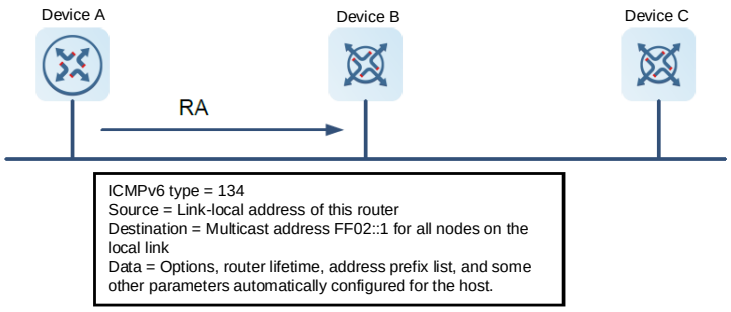
5. Router Discovery/Prefix and Parameter Discovery

RA packets are sent by the device to all link-local nodes on a regular basis. From the RA packets received, the nodes obtain neighbor router information and other configuration parameters. This is called router discovery/prefix and parameter discovery.

The nodes automatically configure the IPv6 address based on the information obtained from router discovery/prefix discovery, which is called stateless auto-configuration.

The RA packet sending process during router discovery/prefix and parameter discovery is shown in the following figure:

Figure 1-17 Router Discovery/Prefix and Parameter Discovery



6. Redirection

If a router receiving an IPv6 packet finds a better next hop, it sends an ICMP Redirect packet to inform the host of the better next hop. The host will directly send the IPv6 packet to the better next hop next time. This function is the same as ICMP Redirect packets of IPv4.

1.3.5 Protocols and Standards

- RFC4291: IPv6 Addressing Architecture.
- RFC2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC4861: Neighbor Discovery for IP version 6 (IPv6)
- RFC4862: IPv6 Stateless Address Autoconfiguration
- RFC5059: Deprecation of Type 0 Routing Headers in IPv6

1.4 Configuring IPv6 Basic Information

1.4.1 Overview

IPv6 is updated from IPv4 and solves many shortcomings of the IPv4.

The most significant difference between IPv6 and IPv4 is the upgrade of the IP address length from 32 bits to 128 bits. IPv6 features simplified header format, adequate address space, hierarchical address structure, flexible extension headers, and enhanced neighbor discovery mechanism and will be full of vitality in the future market competition.

1.4.2 Configuration Task Summary

The IPv6 basic configuration includes the following tasks:

(1) Configuring an IPv6 Address

(2) (Optional) Configuring the IPv6 MTU for an Interface

(3) (Optional) Configuring IPv6 Source Routing

(4) (Optional) Configuring the IPv6 Hop Limit

(5) (Optional) Configuring the Default Gateway for a Management Interface

(6) Configure the sending of ICMPv6 packets. The following configuration tasks are optional. Select either of them for configuration according to the actual condition.

- Configuring the Specified Source Address for Sending ICMPv6 Packets
- Configuring the Transmission Rate of ICMPv6 Error Messages

1.4.3 Configuring an IPv6 Address

1. Overview

This section describes how to enable an interface to support the IPv6 protocol, and configure an IPv6 address for the interface to achieve IPv6 network communication.

The IPv6 link-local address can be manually configured or automatically obtained.

2. Restrictions and Guidelines

- Anycast addresses cannot be configured as interface IPv6 addresses. Exceptionally, anycast addresses with a subnet prefix of 127 or greater can be configured.
- If an interface is bound to a multiprotocol virtual routing and forwarding (VRF) instance not configured with IPv6 address family, IPv6 cannot be enabled on this interface or an IPv6 address cannot be configured for this interface. You can enable IPv6 or configure an IPv6 address for this interface only after configuring an IPv6 address family for the multiprotocol VRF instance.
- IPv6 can be enabled on an interface by two methods: (1) Run the **ipv6 enable** command in interface configuration mode by referring to Step (4); (2) Configure an IPv6 address for the interface by referring to Step (5). If an IPv6 address is configured on an interface, IPv6 is automatically enabled on this interface. In this case, IPv6 cannot be disabled even when you run the **no ipv6 enable** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) (Optional) Enable IPv6 on the interface.

ipv6 enable

IPv6 is disabled on an interface by default.

(5) Configure an IPv6 address for the interface. The configuration steps below are mutually exclusive. Please configure only one task.

- Manually configure an IP address for the interface.

  ipv6 address { *ipv6-address/prefix-length* | *ipv6-prefix/prefix-length* **eui-64** | *prefix-name sub-bits/prefix-length* [**eui-64**] }

  No IPv6 address is configured by default.

If an IPv6 interface is created and is in up state, the system automatically generates a link-local address for this interface.

- Use the general prefix mechanism to generate an IPv6 address for the interface.

  ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

  No IPv6 general prefix is configured by default.

- Enable the IPv6 stateless address auto-configuration on the interface.

  ipv6 address autoconfig

  The IPv6 stateless address auto-configuration is disabled on an interface by default.

1.4.4 Configuring the IPv6 MTU for an Interface

1. Overview

IPv6 PMTUD allows a host to dynamically discover the MTU size on the data path. When sending an IPv6 packet, a host compares the IPv6 MTU of the outbound interface with the PMTU and determines which MTU is smaller. If the packet length is greater than the smaller MTU, the host fragments the packet based on the smaller MTU.

2. Restrictions and Guidelines

The IPv6 MTU of an interface must be less than or equal to the interface MTU.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the IPv6 MTU for the Interface.

ipv6 mtu *bytes*

The IPv6 MTU value is the same as the value configured by running the **mtu** command on an interface by default.

1.4.5 Configuring IPv6 Source Routing

1. Overview

Similar to the IPv4 loose source routing and loose record routing options, the IPv6 routing header is used to specify the intermediate nodes that the packet passes through.

2. Restrictions and Guidelines

Since the Type 0 routing header may cause the device vulnerable DoS attacks, the device does not forward IPv6 packets carrying the routing header by default, but still processes IPv6 packets that are finally destined to itself and carry the Type 0 routing header.

An administrator can run the **ipv6 source-route** command in global configuration mode to enable IPv6 source routing.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configures the device to forward IPv6 packets carrying the routing header.

ipv6 source-route

IPv6 packets carrying the routing header are not forwarded by default.

1.4.6 Configuring the IPv6 Hop Limit

1. Overview

This section describes how to configure the hop limit for unicast packets to prevent infinite transmission of the packets on the network.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the hop limit for unicast packets.

ipv6 hop-limit *hop*

The default hop limit for unicast packets is 64.

1.4.7 Configuring the Default Gateway for a Management Interface

1. Overview

This section describes how to configure the default gateway for a management interface. After configuration, a default route is generated, with the outbound interface of the management interface and the next hop of the configured gateway.

2. Restrictions and Guidelines

This command can be configured on management interfaces only.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface mgmt *interface-number*

(4) Configure the default gateway for the management interface.

ipv6 gataway *ipv6-address*

No IPv6 default gateway is configured for a management interface by default.

1.4.8 Configuring the Specified Source Address for Sending ICMPv6 Packets

1. Overview

In a network with a large number of IPv6 addresses configured, it is complex for receivers to recognize the device, from which an ICMPv6 packet is sent. To simplify the judgment, you can configure a specified source address for ICMPv6 packets.

2. Restrictions and Guidelines

You can configure a specified address, like the address of the loopback interface, as the source address of ICMPv6 packets to simplify judgment.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a specified source address for sending ICMPv6 packets.

ipv6 icmp source [**vrf** *vrf-name*] *ipv6-address*

No address is configured as the specified source address for sending ICMPv6 packets by default.

1.4.9 Configuring the Transmission Rate of ICMPV6 Error Messages

1. Overview

When receiving an invalid IPv6 packet, a device will discard the packet and send an ICMPv6 error message to the source IPv6 address. When attacked by a large number of invalid IPv6 packets, the device continuously replies with ICMPv6 error messages till resources are exhausted and thereby fail to properly provide services. This is called DoS attacks. To prevent DoS attacks, you can restrict the transmission rate of ICMPv6 error messages.

If the length of an IPv6 packet to be forwarded exceeds the IPv6 MTU of the outbound interface, the router discards this IPv6 packet and sends an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used for IPv6 PMTUD. When there are too many ICMPv6 error messages, the ICMPv6 Packet Too Big message may be filtered out, causing the failure of the IPv6 PMTUD function. To avoid this problem, you are advised to restrict the transmission rates of the ICMPv6 Packet Too Big message and other ICMPv6 error messages separately.

Note

Although ICMPv6 Redirect packets are not a type of ICMPv6 error messages, the device restricts their rates together with other ICMPv6 error messages except Packet Too Big messages.

2. Restrictions and Guidelines

Since the precision of the timer is 10 milliseconds, you are advised to set the refresh cycle of a token bucket to an integer multiple of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the refresh rate is set to send one packet within the refresh cycle of 5 milliseconds, the refresh rate that actually takes effect is that two packets are sent within the refresh cycle of 10 milliseconds. If the refresh cycle is not an integral multiple of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted into an integral multiple of 10 milliseconds. For example, if the refresh rate is set to send three packets within the refresh cycle of 15 milliseconds, the refresh rate that actually takes effect is that two packets are sent within the refresh cycle of 10 milliseconds.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the transmission rate of the ICMPv6 Too Big message.

ipv6 icmp error-interval too-big *interval* [*bucket-size*]

Ten messages are transmitted within 100 ms by default.

(4) Configure the transmission rate of other ICMPv6 error messages.

ipv6 icmp error-interval *interval* [*bucket-size*]

Ten messages are transmitted within 100 ms by default.

1.5 Configuring IPv6 NDP

1.5.1 Overview

Neighbor Discovery Protocol (NDP) is a basic part of IPv6. Its main functions include router discovery, prefix discovery, parameter discovery, address auto-configuration, address resolution (like ARP), next-hop determination, neighbor unreachability detection (NUD), duplicate address detection (DAD), and redirection.

1.5.2 Configuration Task Summary

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring a Static Neighbor Entry
- Configuring ND Entry Management
- Configuring Address Resolution
- Configuring NUD
- Configuring DAD
- Configuring Redirection
- Configuring Parameters Related to RA Packets
- Configuring ND Logging

- Configuring the Interval for ND Packet Rate Statistics Collection
- Configuring Local ND Proxy
- Restraining an Interface from Sending NS Packets to Authenticated VLANs
- Configuring the ND Protocol to Allocate Different Prefixes to Different Users
- Configuring Local ND Proxy

1.5.3 Configuring a Static Neighbor Entry

1. Overview

A static neighbor entry is uniquely identified by the IPv6 address of a neighbor node and the ID of an L3 interface connected to this neighbor node.

2. Restrictions and Guidelines

A static neighbor entry can be configured on IPv6-enabled interfaces only. If the neighbor entry to be configured is learned through NDP and stored in the neighbor table, the dynamic neighbor entry will be automatically converted into a static one. An effective static neighbor entry will be always reachable. An invalid static neighbor entry refers to a static neighbor entry with the configured IPv6 address not matching the address configured on the interface (not within any IPv6 network segment of this interface, or in conflict with the address of this interface). In this case, packets will not be forwarded through the MAC address specified in the static neighbor entry.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static neighbor entry.

ipv6 neighbor *ipv6-address interface-type interface-number mac-address*

No static neighbor entry is configured by default.

1.5.4 Configuring ND Entry Management

1. Overview

- You can restrict the number of ND entries learned by an interface to prevent malicious neighbor learning attacks. If this number is not restricted, a large number of ND entries will be generated on the device, occupying excessive memory space and affecting forwarding performance.
- You can restrict the number of unresolved ND entries to prevent malicious scanning attacks from causing the generation of a large number of unresolved ND entries and occupying entry resources.
- You can configure the maximum number of ND options to prevent forged ND packets from carrying unlimited ND options and occupying excessive CPU space on the device.
- When an interface is enabled to learn ND entries via DAD NS packets, the interface will create ND entries in stale state when receiving the DAD NS packets.

2. Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring the Maximum Number of ND Entries That Can Be Learned
- Configuring the Maximum Number of Unresolved ND Entries
- Configuring the Maximum Number of ND Options That Can Be Processed
- Enabling an Interface to Learn ND Entries via DAD NS Packets

3. Restrictions and Guidelines

By default, a general interface is disabled to learn ND entries via DAD NS packets but interfaces in a super VLAN are allowed to do so.

4. Configuring the Maximum Number of ND Entries That Can Be Learned

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum number of ND entries that can be learned by an interface.

ipv6 nd cache interface-limit *limit*

The number of neighbor cache entries that can be learned by an interface is not limited by default.

The configured value must be equal to or greater than the number of the neighbor cache entries learned by the current interface. Otherwise, the configuration does not take effect. The configuration is subject to the ND entry capacity supported by the device.

5. Configuring the Maximum Number of Unresolved ND Entries

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum number of unresolved ND entries.

ipv6 nd unresolved *number*

The default maximum number of unresolved ND entries is 0, indicating no restriction. The number is only subject to the ND entry capacity supported by the device.

6. Configuring the Maximum Number of ND Options That Can Be Processed

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) (Optional) Configure the maximum number of ND options that can be processed.

ipv6 nd max-opt *option*

The device supports 10 ND options by default.

7. Enabling an Interface to Learn ND Entries via DAD NS Packets

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the interface to learn ND entries via DAD NS packets.

ipv6 nd dad learning enable

The function of learning ND entries via DAD NS packets by an interface is disabled by default.

1.5.5 Configuring Address Resolution

1. Overview

When a node attempts to communicate with another, the node has to obtain the link-layer address of the peer by sending an NS packet to the peer. In this packet, the destination address is the solicited-node multicast address corresponding to the IPv6 address of the destination node. This packet also contains the link-layer address of the source node. After receiving this NS packet, the destination node replies with an NA packet, in which the destination address is the source address of the NS packet and the content is the link-layer address of the solicited node. After receiving the NA packet, the source node can communicate with the destination node.

2. Restrictions and Guidelines

If the device is configured to actively send an NS packet to a specific VLAN in a super VLAN, then it will only send the NS packet to the VLAN specified in the super VLAN.

If an authentication-exempt VLAN is configured but the authentication-exempt VLAN is not in the VLAN list, NS packets will not be actively broadcast to the authentication-exempt VLAN.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configures a device not to forcibly use the link-local address as the source address when NS packets are sent.

no ipv6 ns-linklocal-src

The link-local address is always used as the source address for sending NS packets by default.

(4) (Optional) Configure the device to actively send NS packets to specific VLANs in the super VLAN.

ipv6 nd resolve vlan { *vlan-list* | **none** }

A device does not actively send NS packets to a specific VLAN in a super VLAN by default.

(5) (Optional) Enter the interface configuration mode.

interface *interface-type interface-number*

(6) Configure the NS packet retransmission interval.

ipv6 nd ns-interval *interval*

The default NS packet retransmission interval on an interface is 0 (indicating unspecified) when the interval is to be filled in the RA packets, and 1,000 ms when the interval is used to control the interval for sending NS packets.

1.5.6 Configuring NUD

1. Overview

If the duration in which a neighbor is considered reachable or the neighbor is in stale state has elapsed but an IPv6 unicast packet needs to be sent to the neighbor, the device performs NUD.

2. Restrictions and Guidelines

A shorter duration in which a neighbor is considered reachable or in stale state indicates that the device detects unreachable neighbors more quickly but more network bandwidth and device resources will be consumed. Therefore, you are not advised to set the duration to a very small value.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the duration in which a neighbor is considered reachable.

pv6 nd reachable-time *time*

By default, the value in an RA packet is 0 (indicating unspecified), and the duration in which a neighbor is considered reachable in neighbor discovery is 30,000 ms.

(5) (Optional) Configure the duration in which a neighbor keeps in stale state.

ipv6 nd stale-time *time*

The default duration of a neighbor in stale state is 1 hour.

1.5.7 Configuring DAD

1. Overview

You need to enable DAD before configuring an IPv6 address for an interface. At this moment, the address is in tentative state. If no address conflict is detected by DAD, this address can be correctly used. If an address conflict is detected and the interface ID of this address is an EUI-64 ID, duplicate link-layer addresses exist on this link. In this case, the system automatically disables this interface to prevent IPv6-related operations on this interface. At the time, you must configure a new address for the interface and disable and then enable the interface to start DAD again.

The software will retry DAD on a conflicting address according to the configured number of NS packets to be sent consecutively and interval. If no address conflict is detected, this address can be normally used.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the number of NS packets to be sent consecutively during DAD.

ipv6 nd dad attempts *attempts*

The default number of NS packets to be sent consecutively during DAD is 1.

(5) Configure the DAD interval.

ipv6 nd dad retry *retry*

The default DAD interval is 1s.

1.5.8 Configuring Redirection

1. Overview

If a router receiving an IPv6 packet finds a better next hop, it sends an ICMP Redirect packet to inform the host of the better next hop. The host will directly send the IPv6 packet to the better next hop next time. ICMPv6 redirection has the same function as ICMP Redirect packets of IPv4.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the IPv6 redirection function on the interface.

ipv6 redirects

The IPv6 redirection function is enabled on an interface by default.

1.5.9 Configuring Parameters Related to RA Packets

1. Overview

An RA packet is a reply to an RS packet and advertises prefix options and certain flag bits.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the sending of RA packets on this interface.

no ipv6 nd suppress-ra

No RA packets are sent by an IPv6 interface by default.

(5) (Optional) Configure the address prefix to be advertised in an RA packet.

ipv6 nd prefix { *ipv6-prefix/prefix-length* | **default** } [[*valid-lifetime* { **infinite** | *preferred-lifetime* }] | [**at** *valid-date preferred-date*] | [**infinite** { **infinite** | *preferred-lifetime* }]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**] | [**pool** *pool-name*] | [**preference** { *high* | *medium* | *low* }] [**proxy**]]

By default, the prefix in an RA packet to be sent by an interface is the prefix configured using the **ipv6 address** command on the interface.

(6) (Optional) Configure the hop limit for RA packets to be sent by the interface.

pv6 nd ra-hoplimit *ra-hoplimit*

The default hop limit of RA packets is 64.

(7) (Optional) Configure the interval for sending RA packets on an interface.

ipv6 nd ra-interval { *interval* | **min-max** *min-interval max-interval* }

The default interval is 200s. The actual interval for sending packets will fluctuate around 200s by ±20%.

(8) (Optional) Configure the MTU for RA packets to be sent by the interface.

ipv6 nd ra-mtu *ra-mtu*

The default MTU of RA packets is the IPv6 MTU value of a network interface.

(9) Configure related parameters of RA packets. All the configuration steps below are optional. Select the configuration steps as required.

- Configure the **Managed address configuration** flag bit in an RA packet.

  ipv6 nd managed-config-flag

  The **Managed address configuration** flag bit in an RA packet is not configured by default.

  The settings of the flag bit determine whether a host receiving this RA packet obtains an address through stateful auto-configuration. If this flag bit is configured, an address will be obtained through

stateful address auto-configuration. Otherwise, an address will not be obtained through stateful address auto-configuration.

- Configure the **Other stateful configuration** flag bit in an RA packet.

  ipv6 nd other-config-flag

  The **Other stateful configuration** flag bit in an RA packet is not configured by default.

  When this flag bit is set, the flag bit in an RA packet sent by the device is set to 1. A host receiving this flag bit uses DHCPv6 to obtain other information except the IPv6 address for auto-configuration.

  When **Managed address configuration** is set, **Other stateful configuration** is also set by default.

- Configure the address of the DNS recursive resolution server contained in an RA packet. Run the following commands in turn.

  no ipv6 nd ra dns server suppress

  The RDNSS option is not carried in an RA packet by default.

  ipv6 nd ra dns server *ipv6-address* { *valid-lifetime* | **infinite** } **sequence** *number*

  The address of the DNS recursive resolution server in an RA packet is not configured by default.

- Configure the DNS suffix in an RA packet. Run the following commands in turn.

  no ipv6 nd ra dns search-list suppress

  The DNSSL option is not carried in an RA packet by default.

  ipv6 nd ra dns search-list *ipv6-domain-name* { *valid-lifetime* | **infinite** } **sequence** *number*

  The DNS suffix contained in an RA packet is not configured by default.

- Configure the router lifetime in an RA packet.

  ipv6 nd ra-lifetime *lifetime*

  The default router lifetime in an RA packet is 1,800 seconds.

- Configure the URL address of an RA packet.

  ipv6 nd ra-url [*ra-url*]

  The URL address of an RA packet is not configured by default.

- Configure the URL option type value in an RA packet.

  ipv6 nd ra-url *type*

  The URL option type value in an RA packet is not configured by default.

1.5.10 Configuring ND Logging

1. Overview

After ND logging is configured, system logs about ND packets received and sent by the device will be printed.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable ND logging.

ipv6 nd log enable

ND logging is disabled by default.

(4) Configure ND logging rate.

ipv6 nd log rate *rate*

20 ND logs are printed per minute by default.

1.5.11 Configuring the Interval for ND Packet Rate Statistics Collection

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the interval for ND packet rate statistics collection.

ipv6 nd packet rate-statistics interval *interval*

The ND packet rate statistics collection is disabled by default.

1.5.12 Configuring Local ND Proxy

1. Overview

After local ND proxy is enabled on an interface, when receiving NS messages that request addresses of other hosts, the device replies with NA messages containing its MAC address.

If L2 access isolation or inter-subnet isolation (such as sub VLANs) is configured, after local ND proxy is enabled on the gateway, the gateway serves as a proxy to process NS packets from the downlink users and replies with NA packets containing the gateway's MAC address. Thus, the traffic of communication among these users is forwarded by the gateway at L3.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable local ND proxy.

local-proxy-nd enable [**force**]

Local ND proxy is disabled on an interface by default.

1.5.13 Configuring the ND Protocol to Allocate Different Prefixes to Different Users

1. Overview

A specific prefix pool can be configured on an interface so that the device assigns different IPv6 prefixes to different users served by the interface.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a prefix pool for prefix allocation.

ipv6 local pool *pool-name prefix/prefix-length assigned-length*

No local prefix pool is configured for DHCPv6 server prefix proxy by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure the name of the prefix pool bound to the interface.

ipv6 nd prefix pool *pool-name*

No prefix pool is bound to an interface by default.

1.5.14 Restraining an Interface from Sending NS Packets to Authenticated VLANs

1. Overview

In gateway authentication mode, all sub VLANs in a super VLAN are authenticated VLANs by default. Users in an authenticated VLAN have to pass authentication to access the network. After authentication, a static ND entry is generated on the device. Therefore, when accessing an authenticated user, the device does not need to send NS packets to the authenticated VLAN. If the device attempts to access users in an authentication-exempt VLAN, it only needs to send ARP requests to the authentication-exempt VLAN.

In gateway authentication mode, the function of restraining from sending NS packets to authenticated VLANs is enabled on the device by default. If the device needs to access non-authenticated users in an authenticated VLAN, disable this function.

2. Restrictions and Guidelines

The configuration is supported only on SVIs and takes effect only in gateway authentication mode.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Restrain the interface from sending NS packets to authentication-exempt VLANs.

ipv6 nd suppress-auth-vlan-ns

NS packets are not sent to authenticated VLANs by default.

1.6 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** command to clear information.

Caution

Running the **clear** command may lose vital information and thus interrupt services.

Table 1-3 IPv6 Monitoring

Command	Purpose
clear ipv6 neighbors [**vrf** *vrf-name*] [**oob**] [*interface-type interface-number*]	Clears the dynamically learned neighbor entries.
show ipv6 address [*interface-type interface-number*]	Displays IPv6 addresses.
show ipv6 general-prefix	Displays the prefix information in a general prefix.
show ipv6 nd [**interface** *interface-type interface-number*] **statistics**	Displays the statistics on IPv6 ND packets.
show ipv6 neighbors [**vrf** *vrf-name*] **statistics** [**all**]	Displays the statistics on IPv6 neighbor tables.
show ipv6 packet statistics [**total** | *interface-type interface-number*]	Displays the statistics on IPv6 packets.
show ipv6 neighbors [**vrf** *vrf-name*] [**verbose**] [*interface-type interface-number*] [*ipv6-address*] [**static**] [**oob**]	Displays neighbor information.
show ipv6 raw-socket [*protocol*]	Displays all IPv6 raw sockets
show ipv6 routers [*interface-type interface-number*]	Displays the neighbor router information and RA packets.
show ipv6 sockets	Displays all IPv6 sockets.
show ipv6 udp [**local-port** *port-number*] [**peer-port** *port-number*]	Displays all IPv6 UDP sockets.
show ipv6 udp statistics	Displays the statistics on IPv6 UDP sockets.

Command	Purpose
show ipv6 interface [[*interface*-type interface-number] [**ra-info**] | **brief** [*interface-type interface-number*]]	Displays the information about IPv6 interfaces.

1.7 Configuration Examples

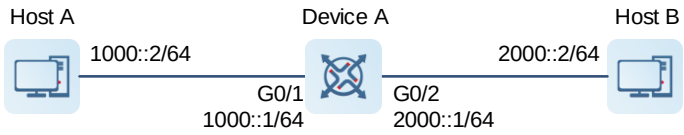
1.7.1 Manually Configuring IPv6 Addresses

1. Requirements

Host A and host B communicate with each other through IPv6 addresses.

2. Topology

Figure 1-18 Topology of IPv6 Addresses



3. Notes

Enable IPv6 on an interface and configure an IPv6 address.

4. Procedure

(1) Configure device A.

Configure an IPv6 address for port GigabitEthernet 0/1 and enable the sending of RA packets on this interface.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 enable
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 address 1000::1/64
DeviceA(config-if-GigabitEthernet 0/1)# no ipv6 nd suppress-ra
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Configure an IPv6 address for port GigabitEthernet 0/2 and enable the sending of RA packets on this interface.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 enable
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 address 2000::1/64
DeviceA(config-if-GigabitEthernet 0/1)# no ipv6 nd suppress-ra
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

(2) Configure hosts.

Set the IPv6 address of host A to 1000::2/24.

Set the IPv6 address of host B to 2000::2/24.

5. Verification

Run the **show ipv6 interface** command to check that IPv6 addresses are successfully added to the interfaces.

```
DeviceA# show ipv6 interface

interface GigabitEthernet 0/1 is Up, ifindex: 2, vrf_id 0
  address(es):
    Mac Address: 00:50:56:b0:05:99
    INET6: FE80::250:56FF:FEB0:599 , subnet is FE80::/64
    INET6: 1000::1 , subnet is 1000::/64
  Joined group address(es):
    FF01::1
    FF02::1
    FF02::2
    FF02::1:FF00:0
    FF02::1:FF00:1
    FF02::1:FFB0:599
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND stale time is 3600 seconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 600 seconds<480--720>
  ND router advertisements live for 1800 seconds

interface GigabitEthernet 0/2 is Down, ifindex: 3, vrf_id 0
  address(es):
    Mac Address: 00:50:56:b0:05:9a
    INET6: FE80::250:56FF:FEB0:59A [ TENTATIVE ], subnet is FE80::/64
    INET6: 2000::1 [ TENTATIVE ], subnet is 2000::/64
  Joined group address(es):
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND stale time is 3600 seconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 600 seconds<480--720>
```

```
 ND router advertisements live for 1800 seconds
```

On host A, run the **ping** command to test the interconnectivity with host B.

On host B, run the **ping** command to test the interconnectivity with host A

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
interface gigabitethernet 0/1
ipv6 enable
ipv6 address 1000::1/64
no ipv6 nd suppress-ra
!
interface gigabitethernet 0/2
ipv6 enable
ipv6 address 2000::1/64
no ipv6 nd suppress-ra
!
```

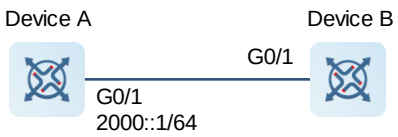
1.7.2 Enabling Stateless IPv6 Address Auto-configuration

1. Requirements

Device A is connected to device B through the GigabitEthernet 0/1 interface which is configured with an IPv6 address. Stateless address auto-configuration needs to be configured on device B to obtain an IPv6 address so that the two devices can communicate with each other through the IPv6 addresses.

2. Topology

Figure 1-19 Topology of Stateless IPv6 Address Auto-configuration



3. Notes

- Configure an IPv6 address on device A.
- Enable stateless address auto-configuration on device B to obtain an IPv6 address.

4. Procedure

(1) Configure device A.

Configure an IPv6 address for port GigabitEthernet 0/1 and enable the sending of RA packets on this interface.

```
DeviceA> enable
DeviceA# configure terminal
```

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 address 2000::1/64
DeviceA(config-if-GigabitEthernet 0/1)# no ipv6 nd suppress-ra
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

(2) Configure device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ipv6 address autoconfig
```

5. Verification

On device B, run the **show ipv6 interface** command to check that the interface automatically obtains an IPv6 address.

```
DeviceB# show ipv6 interface

interface GigabitEthernet 0/1 is Up, ifindex: 2, vrf_id 0
  address(es):
    Mac Address: 00:50:56:b0:2f:50
    INET6: FE80::250:56FF:FEB0:2F50 , subnet is FE80::/64
    INET6: 2000::250:56FF:FEB0:2F50 [ PRE ], subnet is 2000::/64
      valid lifetime 2591906 sec, preferred lifetime 604706 sec
  Joined group address(es):
    FF01::1
    FF02::1
    FF02::2
    FF02::1:FF00:0
    FF02::1:FFB0:2F50
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND stale time is 3600 seconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 600 seconds<480--720>
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

On device A, run the **ping** command to test the interconnectivity with device B.

```
DeviceA# ping ipv6 2000::250:56FF:FEB0:2F50
Sending 5, 100-byte ICMP Echoes to 2000::250:56ff:feb0:2f50, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/13/63 ms.
```

On device B, run the **ping** command to test the interconnectivity with device A.

```
DeviceAB# ping ipv6 2000::1
Sending 5, 100-byte ICMP Echoes to 2000::1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface gigabitEthernet 0/1
ipv6 enable
ipv6 address 2000::1/64
no ipv6 nd suppress-ra
!
```

- Device B configuration file

```
hostname DeviceB
!
interface gigabitEthernet 0/1
ipv6 address autoconfig
!
```

Contents

1 Configuring DHCPv6 1
1.1 Introduction 1
1.2 Principles 1
1.2.1 Basic Concepts 1
1.2.2 Packet Format 4
1.2.3 Requesting/Allocating Addresses 4
1.2.4 Requesting/Allocating Prefixes 8
1.2.5 Stateless Service 9
1.2.6 DHCPv6 Relay Agent 9
1.2.7 Address Advertisement 11
1.2.8 Protocols and Standards 12
1.3 Restrictions and Guidelines 12
1.4 Configuration Task Summary 12
1.5 Configuring the DHCPv6 Server to Assign Addresses 12
1.5.1 Overview 12
1.5.2 Configuration Tasks 12
1.5.3 Configuring the IA_NA Address Prefix to Be Assigned from a DHCPv6 Server to a DHCPv6 Client 13
1.5.4 Configuring the Prefix of a Statically Bound Address to Be Assigned from a DHCPv6 Server to a DHCPv6 Client 13
1.5.5 Configuring a DCHPv6 Server to Assign Prefixes from a Local Prefix Pool 13
1.5.6 Configuring Excluded Addresses on a DHCPv6 Server 14
1.5.7 Enabling the DHCPv6 Server Service 14

1.6 Configuring the DHCPv6 Server to Assign Other Network Parameters 14

1.6.1 Overview 14

1.6.2 Configuration Tasks 14

1.6.3 Configuring the DNS Address to Be Assigned from a DHCPv6 Server to a DHCPv6 Client 15

1.6.4 Configuring the Domain Name to Be Assigned from a DHCPv6 Server to a DHCPv6 Client 15

1.6.5 Configuring the Boot File URL to Be Assigned from a DHCPv6 Server to a DHCPv6 Client 15

1.6.6 Configuring Option 52 on a DHCPv6 Server 16

1.7 Configuring the DHCPv6 Relay 16

1.7.1 Overview 16

1.7.2 Restrictions and Guidelines 16

1.7.3 Procedure 16

1.8 Configuring Source Interface Designation Function on a DHCPv6 Relay Agent 17

1.8.1 Overview 17

1.8.2 Restrictions and Guidelines 17

1.8.3 Procedure (Global Configuration Mode) 17

1.8.4 Procedure (Interface Configuration Mode) 18

1.9 Monitoring 18

1.10 Configuration Examples 19

1.10.1 Dynamically Assigning IPv6 Addresses 19

1.10.2 Dynamically Assigning IPv6 Address Prefixes 21

1.10.3 Configuring DHCP Relay 24

1 Configuring DHCPv6

1.1 Introduction

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is a protocol that allows a DHCPv6 server to transfer configurations to IPv6 nodes, such as IPv6 address, domain name server (DNS) address, network information service (NIS) server address, and Simple Network Time Protocol (SNTP) server address.

Compared with other IPv6 address assignment methods, such as manual configuration and Stateless Address Autoconfiguration (SLAAC), DHCPv6 has the following advantages:

- DHCPv6 provides the address assignment, prefix delegation (PD), and configuration parameter allocation functions.
- DHCPv6 is a Stateful Address Autoconfiguration (SAAC) protocol for flexibly adding and reusing network addresses. It can record assigned addresses, which enhances network manageability.
- By using DHCPv6 PD, uplink network devices can assign address prefixes to downlink network devices, ensuring flexible station-level automatic configuration and flexible control of station address space.
- DHCPv6 configuration parameter allocation solves the problem that parameters cannot be obtained through the SLAAC protocol and allows a DHCPv6 server to assign DNS addresses and domain names to hosts.
- DHCPv6 is a protocol based on the client/server model. A DHCPv6 client is used to obtain various configurations, whereas a DHCPv6 server is used to provide various configurations. If the DHCPv6 client and DHCPv6 server are not on the same network link, they can interact with each other by using a DHCPv6 relay.

1.2 Principles

1.2.1 Basic Concepts

1. IPv6 address assignment methods

- Manual configuration: IPv6 addresses/prefixes and other network configuration parameters are manually configured.
- SLAAC: A host uses the prefix carried in a received Router Advertisement (RA) message and the local interface ID to automatically generate an IPv6 address.
- SAAC (DHCPv6): DHCPv6 includes the following three types:
  - DHCPv6 SAAC: A DHCPv6 server automatically configures IPv6 addresses/prefixes and other network configuration parameters.
  - DHCPv6 SLAAC: A host automatically generates an IPv6 address by using an RA message. The DHCPv6 server assigns configuration parameters other than IPv6 addresses.
  - DHCPv6 PD: A lower-layer network router applies for a prefix from an upper-layer network router, and the upper-layer network router assigns a proper address prefix to the lower-layer network router. The lower-layer network router automatically divides the delegated prefix (less than 64 bits) into subnet segments with a 64-bit prefix and assigns these prefixes to the links directly connected to IPv6 hosts through RA messages, ensuring automatic address configuration for the hosts.

2. DUID

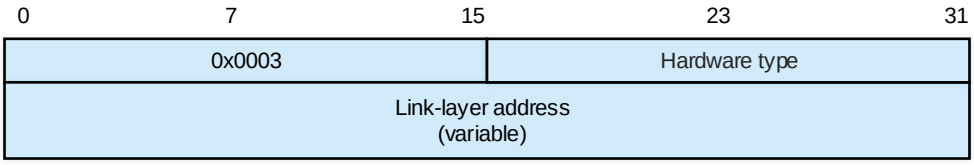
A DHCP Unique Identifier (DUID) uniquely identifies a DHCPv6 device (DHCPv6 client, relay, or server). It is used for mutual authentication during DHCPv6 message exchanges.

RFC 3315 defines three types of DUIDs:

- DUID Based on Link-Layer address plus Time (DUID-LLT)
- DUID Assigned by Vendor Based on Enterprise Number (DUID-EN)
- Link-Layer address (DUID-LL)

Ruijie DHCPv6 devices use DUID-LLs.

Figure 1-1 DUID-LL Structure



DUID type is set to **0x0003**, **Hardware type** is set to **0x0001** (indicating the supported hardware type of Ethernet), and **Link-layer address** is set to the Media Access Control (MAC) address of the interface with the minimum serial number on the device.

3. Multicast address

In DHCP, clients broadcast DHCP packets to servers. To prevent broadcast storms, DHCPv6 uses multicast packets instead of broadcast packets. DHCPv6 uses the following multicast addresses:

- FF02::1:2: a link-scoped multicast address used by a client to communicate with neighboring relay agents and servers. All DHCPv6 servers and relay agents on the link are members of this multicast group.
- FF05::1:3: a site-scoped multicast address used by a DHCPv6 relay agent to communicate with servers. All DHCPv6 servers within the site are members of this multicast group.

4. Identity association (IA)

A DHCPv6 server uses IAs to assign addresses to DHCPv6 clients. Each IA is uniquely identified by an identity association identifier (IAID). IAIDs are generated by DHCPv6 clients. One-to-one mappings are established between IAs and clients. An IA may contain several addresses, which can be allocated by the client to other interfaces. An IA may contain one of the following types of addresses:

- Non-temporary addresses (NAs), namely, globally unique addresses
- Temporary addresses (TAs), which are hardly used
- PD, prefix delegation

Based on the address type, IAs are classified into IA_NA, IA_TA, and IA_PD types. Ruijie DHCPv6 servers support only IA_NA and IA_PD.

5. Binding

A DHCPv6 binding is a manageable address information structure. An address binding on a DHCPv6 server records the IA and other configurations of a client. A client can request multiple bindings. The address binding

data on a server is presented in the form of an address binding table. Bindings that contain IAs use DUID, IA-Type, or IAID as the index, and bindings that contain configurations use DUID as the index.

6. DHCPv6 address pool

A DHCPv6 server uses address pools to save IP addresses and network parameters to be assigned to clients.

7. Sequence for selecting addresses/prefixes

A DHCPv6 server selects to-be-assigned IPv6 addresses/prefixes based on the following sequence:

(1) Addresses/prefixes previously assigned to the client

(2) Idle address/prefixes in the address pool/prefix pool that meet the client's requirements

(3) Other idle addresses/prefixes in the address pool/prefix pool

(4) Expired or previously conflicted addresses/prefixes

(5) If no address is available, the DHCPv6 server does not assign an address to the client.

8. Address conflict

When an address assigned to a DHCPv6 client is conflicted, the client sends a DECLINE packet to notify the DHCPv6 server that the address is rebound. Then, the server adds the address to the address conflict queue. The server does not assign addresses in the address conflict queue to clients, and can display and clear address information in the address conflict queue.

9. Packet type

DHCPv6 uses User Datagram Protocol (UDP) ports 546 and 547 for packet exchanges. Specifically, a DHCPv6 client uses port 546 for receiving packets, while a DHCPv6 server and a DHCPv6 relay agent use port 547 for receiving packets. The following describes types of packets that can be exchanged among a DHCPv6 server, client, and relay agent:

- Packets that may be sent from a DHCPv6 client to a DHCPv6 server include SOLICIT, REQUEST, CONFIRM, RENEW, REBIND, RELEASE, DECLINE, and INFORMATION-REQUEST packets.
- Packets that may be sent from a DHCPv6 server to a DHCPv6 client include ADVERTISE, REPLY, and RECONFIGURE packets.
- Packets that may be sent from a DHCPv6 relay agent to another DHCPv6 relay agent or a DHCPv6 server include RELAY-FORWARD packets.
- Packets that may be sent from a DHCPv6 server or DHCPv6 relay agent to another DHCPv6 relay agent include RELAY-REPLY packets.

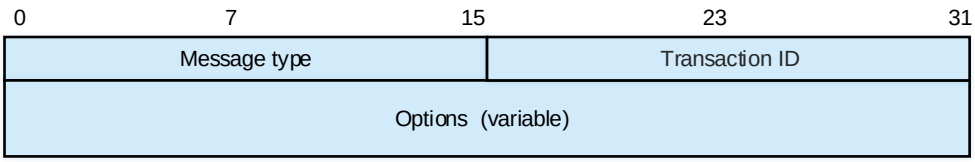
Note

- Ruijie DHCPv6 servers do not support RECONFIGURE packets.
- Ruijie DHCPv6 clients do not support CONFIRM and RECONFIGURE packets.

1.2.2 Packet Format

1. Format of Packets Exchanged Between a DHCPv6 Client and a DHCPv6 Server

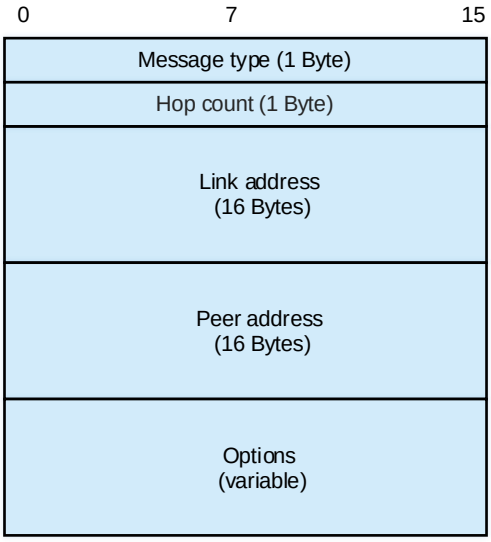
Figure 1-2 Format of Packets Exchanged Between a DHCPv6 Client and a DHCPv6 Server



- **Message type**: Identifies the message type of a DHCPv6 packet.
- **Transaction ID**: Identifies a DHCPv6 packet exchange.
- **Options**: variable-length options carried in a packet.

2. Format of Packets Exchanged Between a DHCPv6 Relay Agent and a DHCPv6 Server

Figure 1-3 Format of Packets Exchanged Between a DHCPv6 Relay Agent and a DHCPv6 Server



- **Message type**: Identifies the message type of a DHCPv6 packet. Only RELAY-FORWARD and RELAY-REPLY packets can be exchanged between a DHCPv6 relay agent and a DHCPv6 server.
- **Hop count**: Number of relays that a packet passes through.
- **Link address**: Used by a DHCPv6 server to identify the access link of a client. It is a global IPv6 unicast address or link-local address.
- **Peer address**: Source address of a relayed packet, that is, the address of a client or a relay agent.
- **Options**: Variable-length options. The **Relay message** option is mandatory, and a relay agent can add other options.

1.2.3 Requesting/Allocating Addresses

A DHCPv6 client can request an IPv6 address from a DHCPv6 server.

After being configured with available addresses, a DHCPv6 server can assign IPv6 addresses to hosts in the network and record the assigned addresses to improve the network manageability.

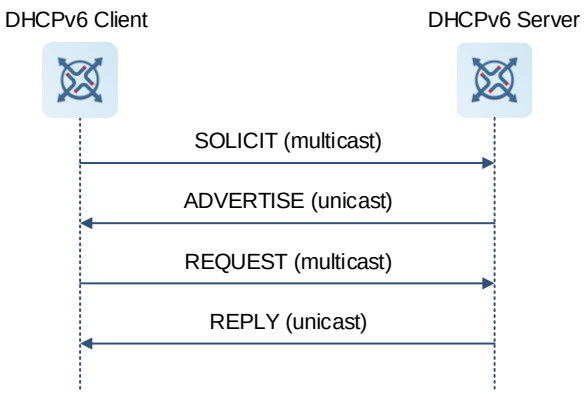
1. Principles

Network hosts serve as DHCPv6 clients and DHCPv6 servers to implement address assignment, update, confirmation, and release through message exchanges.

2. Four-Way Message Exchange

Generally, a DHCPv6 client and a DHCPv6 server implement address, prefix, and parameter configuration through a four-way message exchange.

Figure 1-4 Process of Four-Way Message Exchange



(1) A DHCPv6 client sends a SOLICIT message with the destination address FF02::1:2 and destination port 547 on the local link in multicast mode to request an address, a prefix, and configuration parameters. All DHCPv6 servers or DHCPv6 relay agents on the link receive this SOLICIT message.

(2) After receiving the SOLICIT message, the DHCPv6 server sends an ADVERTISE message in unicast mode if it can provide the information requested in the SOLICIT message. The ADVERTISE message includes the requested address, prefix, and configuration parameters.

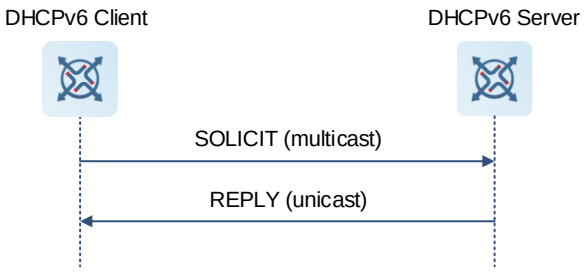
(3) The DHCPv6 client may receive the ADVERTISE messages from multiple DHCPv6 servers. Generally, the DHCPv6 client selects the server from which it first receives the ADVERTISE message as the DHCPv6 server. Then, the DHCPv6 client sends a REQUEST message with the destination address FF02::1:2 and destination port 547 to request an address, a prefix, and configuration parameters.

(4) After receiving the REQUEST message, the DHCPv6 server creates a binding locally and sends a REPLY message in unicast mode. The REPLY message includes the address, prefix and configuration parameters that the DHCPv6 server assigns to the DHCPv6 client. The DHCPv6 client completes address, prefix, or parameter configuration based on the information in the REPLY message.

3. Two-Way Message Exchange

The two-message exchange can be used to complete address, prefix, and parameter configuration for DHCPv6 clients more quickly.

Figure 1-5 Two-Way Message Exchange



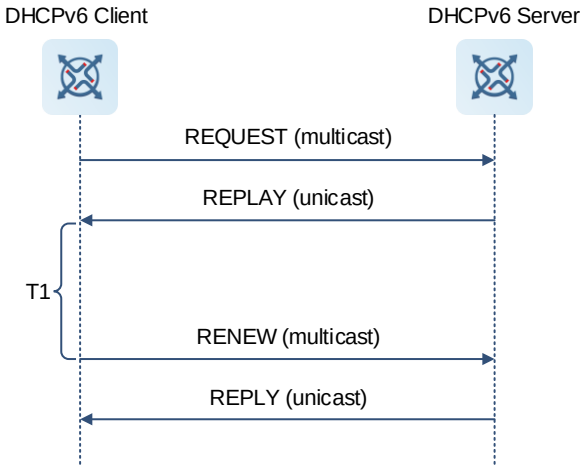
(1) A DHCPv6 client sends a SOLICIT message with the destination address FF02::1:2 and destination port 547 on the local link to request an address, a prefix, and configuration parameters. The SOLICIT message contains the **Rapid Commit** option.

(2) If a DHCPv6 server supports the **Rapid Commit** option, the DHCPv6 server creates a binding locally and sends a REPLY message in unicast mode. The REPLY message includes the address, prefix, and configuration parameters to be assigned to the DHCPv6 client. The DHCPv6 client completes configuration based on the information in the REPLY message. If the DHCPv6 server does not support the **Rapid Commit** option, that is, it does not support rapid assignment, the process of four-way message exchange is used to assign an IPv6 address/a prefix and other network configuration parameters to the client.

4. Update and Rebinding

The DHCPv6 server provides the control address and the updated T1 and T2 in the IA of the REPLY message sent to the DHCPv6 client.

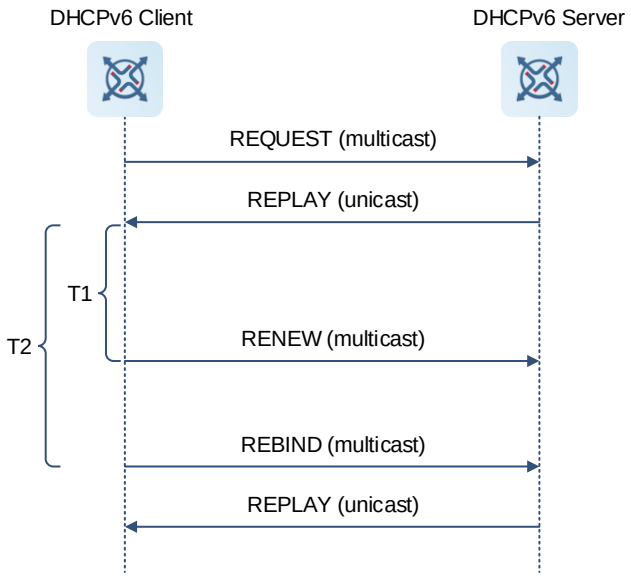
Figure 1-6 Update



(1) The DHCPv6 client sends a RENEW multicast message to the DHCPv6 server for updating the address and prefix after T1 seconds. The RENEW message contains the DUID of the DHCPv6 server and the IA information to be updated.

(2) After receiving the RENEW message, the DHCPv6 server checks whether the DUID value in the RENEW message is the same as its DUID. If yes, the DHCPv6 server updates the local binding and sends a REPLY message in unicast mode. The REPLY message contains the new T1 and other parameters.

Figure 1-7 Rebinding



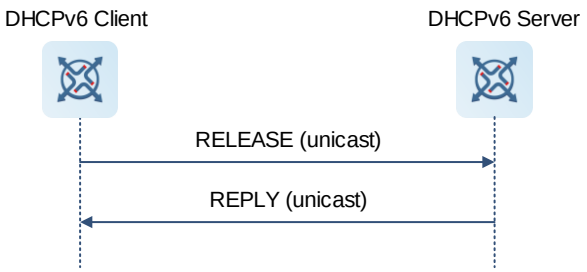
(1) If no response is received within T2 after the DHCPv6 client sends a RENEW message to the DHCPv6 server, the DHCPv6 client sends a REBIND multicast message to the DHCPv6 server for rebinding the address and prefix.

(3) After receiving the REBIND message, the DHCPv6 server (perhaps a new DHCPv6 server) sends a REPLY message based on the content of the REBIND message.

5. Release

If a DHCPv6 client needs to release an address or a prefix, the DHCPv6 client needs to notify the DHCPv6 server of the to-be-released address or prefix. In this way, the DHCPv6 server can assign the address or prefix to other DHCPv6 clients.

Figure 1-8 Release



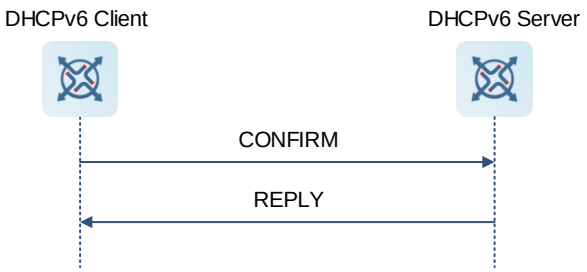
(1) A DHCPv6 client sends a RELEASE message to a DHCPv6 server to notify the DHCPv6 server that it no longer needs to use an address or prefix, that is, to release the address or prefix.

(2) After receiving RELEASE message, the DHCPv6 server removes the corresponding binding based on the address or prefix in the RELEASE message and sends a REPLY message carrying the state option to the DHCPv6 client.

6. Confirmation

After moving to a new link or encountering a restart, a DHCPv6 client needs to confirm whether the original address is still available.

Figure 1-9 Confirmation



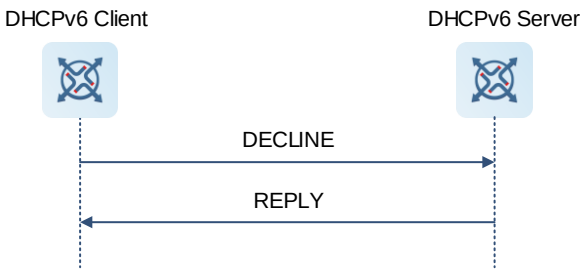
(1) The DHCPv6 client sends a CONFIRM message to the DHCPv6 server on the new link to check whether the original address is still available.

(2) After receiving the CONFIRM message, the DHCPv6 server performs confirmation based on the address information contained in the CONFIRM message and sends a REPLY message carrying the state option to the DHCPv6 client. If the confirmation indicates unavailability, the DHCPv6 client may initiate a new address assignment request.

7. Address conflict

If a DHCPv6 client finds that the assigned address has been occupied on the link, the DHCPv6 client sends a DECLINE message to notify the DHCPv6 server of the address conflict.

Figure 1-10 Address conflict



(1) The DHCPv6 client sends a DECLINE message to the DHCPv6 server. The DECLINE message includes the IA information of the conflicted address.

(2) After receiving the DECLINE message, the DHCPv6 server marks the address in the DECLINE message as **Declined** and does not assign the address to other clients. Then, the DHCPv6 server sends a REPLY message carrying the state option to the DHCPv6 client. You can manually clear addresses marked as **Declined** to facilitate re-assignment.

1.2.4 Requesting/Allocating Prefixes

After available prefixes are configured on a DHCPv6 server, uplink network devices can assign the address prefixes to downlink network devices by serving as the PD of the DHCPv6 server. This ensures flexible station-level automatic address configuration and flexible control of station address space.

Downlink network devices serve as DHCPv6 clients to exchange messages with the DHCPv6 server to implement prefix assignment, update, and release. Downlink network devices obtain, update, rebind, and release prefixes by using the four-way or two-way message exchange mechanism similar to that for assigning addresses. However, prefix assignment is different from address assignment in the following aspects:

- In message exchanges via PD, the CONFIRM and DECLINE messages are not used.
- If a DHCPv6 client connects to a new link and needs to check whether the prefix is available, it performs confirmation by exchanging the REBIND and REPLY messages.
- These messages use IA_PD.

Note

For message exchanges via PD, see section 1.2.3 "Requesting/Allocating Addresses."

1.2.5 Stateless Service

When a DHCPv6 client only needs configuration parameters, the DHCPv6 stateless service can be used to obtain related configuration parameters. This solves the problem that configuration parameters such as the DNS address cannot be obtained through the SLAAC protocol.

Figure 1-11 Message Exchange Using the Stateless Service

(1) A DHCPv6 client sends an INFORMATION-REQUEST message to a DHCPv6 server to request stateless information. Usually, this message does not contain the DUID of a specific DHCPv6 server.

(2) The DHCPv6 server sends a REPLY message containing the configuration parameters to the DHCPv6 client.

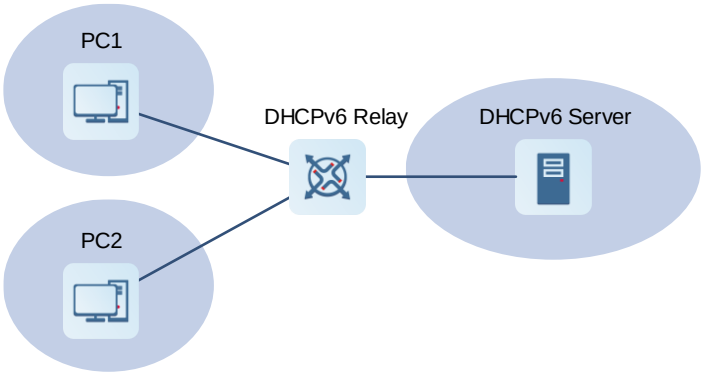
(3) The DHCPv6 client checks whether information provided in the REPLY message is consistent with configuration parameters requested in the INFORMATION-REQUEST message. If yes, the DHCPv6 client performs network configuration based on parameters provided in the REPLY message. Otherwise, it ignores the message. If the DHCPv6 client receives multiple REPLY messages that match the request, the DHCPv6 client completes stateless configuration based on parameters provided in the first received REPLY message.

1.2.6 DHCPv6 Relay Agent

A DHCPv6 client usually discovers a DHCPv6 server by sending Solicit packets with a multicast address as the destination address. Therefore, the DHCPv6 client and DHCPv6 server must be able to directly communicate with each other, that is, they must be deployed on the same link. This may cause inconvenience to management and upgrade and resource waste. The DHCPv6 relay agent function can solve these problems by

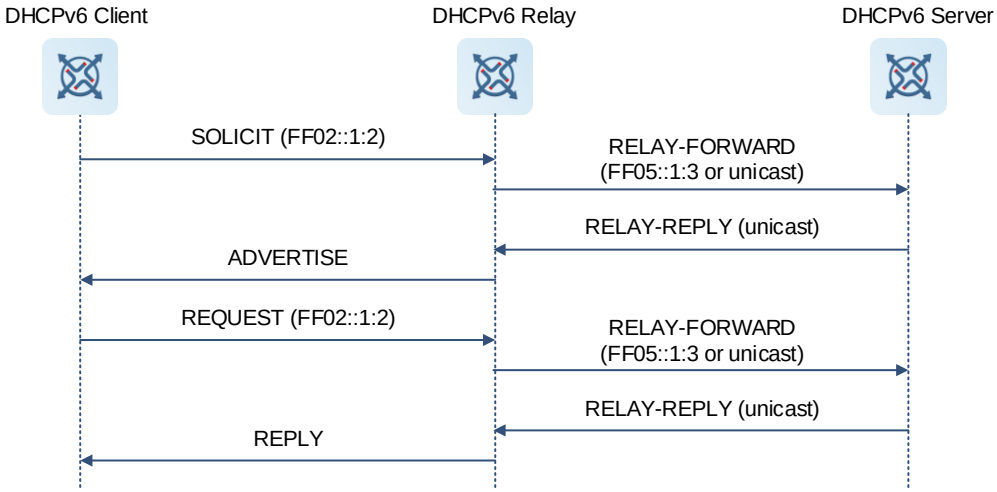
enabling a DHCPv6 client to send packets to a DHCPv6 server on a different link. A DHCP relay agent is often deployed on the link where a DHCPv6 client resides. It is used to forward interaction packets between the DHCPv6 client and a DHCPv6 server. The DHCP relay agent is transparent to the DHCPv6 client.

Figure 1-12 DHCPv6 Relay Agent



2. Principles

Figure 1-13 Packet Exchange Among a DHCPv6 Client, DHCPv6 Relay Agent, and DHCPv6 Server



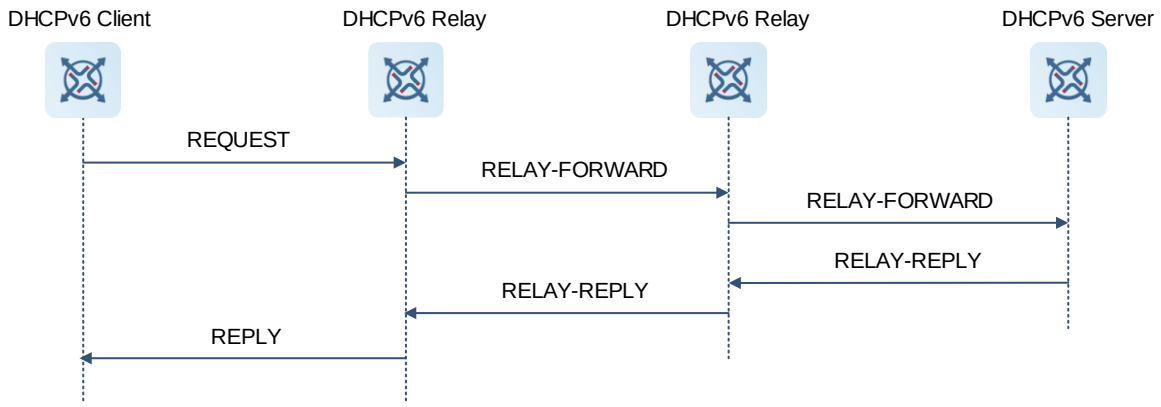
(1) When receiving a SOLICIT or REQUEST message from the DHCPv6 client, a DHCPv6 relay agent creates a RELAY-FORWARD message. This message contains the original message from the DHCPv6 client and some options added by the relay agent. Then, the DHCP relay agent sends the RELAY-FORWARD message to a specified DHCPv6 server or a specific multicast address FF05::1:3.

(2) After receiving the RELAY-FORWARD message, the DHCPv6 server extracts the original message for processing. Then, the DHCPv6 server constructs a response to the original message, encapsulates the response in a RELAY-REPLY message, and sends the RELAY-REPLY message to the DHCPv6 relay agent.

(3) After receiving the RELAY-REPLY message, the DHCPv6 relay agent extracts the original message from the DHCPv6 server and forwards it to the DHCPv6 client.

3. Multi-Level DHCPv6 Relay Agents

Figure 1-14 Multi-Level DHCPv6 Relay Agents



A DHCPv6 relay agent encapsulates and decapsulates messages between a DHCPv6 client and a DHCPv6 server on different links to enable communication between them. Multi-level relay agents are allowed between a DHCPv6 client and a DHCPv6 server.

4. Options Supported by a DHCPv6 Relay Agent

- Interface-ID (Option 18)

  A DHCPv6 relay agent can use **Interface-ID** to identify the interface that receives messages from the client. A DHCPv6 server configures parameters based on the value of **Interface-ID** and copies **Interface-ID** to the RELAY-REPLY message to be sent to the DHCPv6 relay agent. After receiving the RELAY-REPLY message, the DHCPv6 relay agent forwards the message through the interface identified by **Interface-ID**. **Interface-ID** exists only in RELAY-FORWARD and RELAY-REPLY packets.

- Remote-ID (Option 37)

  A DHCPv6 relay agent can use **Remote-ID** to carry the DUID, port, and virtual local area network (VLAN) information. Based on the value of **Remote-ID**, a DHCPv6 server performs address assignment, parameter configuration, and prefix delegation.

- Subscriber-ID (Option 38)

  A DHCPv6 relay agent can use **Subscriber-ID** to carry a client's MAC address and other physical information. Based on the value of **Subscriber-ID**, a DHCPv6 server performs address assignment, parameter configuration, and prefix delegation.

1.2.7 Address Advertisement

A DHCPv6 server advertises a client's IPv6 address and MAC address to the authentication module for auditing.

In a subnet without a DHCPv6 relay, a DHCPv6 server can be configured with the IA_NA address assignment and advertisement functions. When receiving a DHCPv6 packet from a DHCPv6 client, the DHCPv6 server can identify the client's MAC address based on the source MAC address in the packet. When assigning an IPv6 address to the client or renewing the lease of this address, the DHCPv6 server advertises the MAC address and IPv6 address to the authentication module. The authentication module integrates the address information with

IPv4 authentication information of the client and synchronizes the information to the authentication server. The authentication server authenticates or records the client based on the information.

1.2.8 Protocols and Standards

- RFC 3315: Dynamic Host Configuration Protocol for IPv6
- RFC 3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6
- RFC 3646: DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3736: Stateless DHCP Service for IPv6
- RFC 5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

1.3 Restrictions and Guidelines

- To provide the DHCPv6 service, specify a DHCPv6 address pool.
- The DHCPv6 service can be configured only on a Switch Virtual Interface (SVI), L3 Ethernet interface, or L3 aggregate port (AP).

1.4 Configuration Task Summary

DHCPv6 configuration includes the following tasks:

- Configuring the DHCPv6 server
  - a Configuring the DHCPv6 Server to Assign Addresses
  - b (Optional) Configuring the DHCPv6 Server to Assign Other Network Parameters
  - c Configuring the DHCPv6 Server to Assign Other Network Parameters
- Configuring the DHCPv6 relay
  - a Configuring the DHCPv6 Relay
  - d (Optional) Configuring Source Interface Designation Function on a DHCPv6 Relay Agent

1.5 Configuring the DHCPv6 Server to Assign Addresses

1.5.1 Overview

Configure the device as a DHCPv6 server to assign IPv6 addresses or prefixes to DHCPv6 clients.

1.5.2 Configuration Tasks

(1) Configuring the DHCPv6 Server to Assign Addresses Perform either of the following configuration tasks.

- Configuring the IA_NA Address Prefix to Be Assigned from a DHCPv6 Server to a DHCPv6 Client
- Configuring the Prefix of a Statically Bound Address to Be Assigned from a DHCPv6 Server to a DHCPv6 Client
- Configuring a DCHPv6 Server to Assign Prefixes from a Local Prefix Pool

(2) (Optional) Configuring Excluded Addresses on a DHCPv6 Server

(3) Enabling the DHCPv6 Server Service

1.5.3 Configuring the IA_NA Address Prefix to Be Assigned from a DHCPv6 Server to a DHCPv6 Client

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a DHCPv6 address pool and enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure the IA_NA address prefix to be assigned from a DHCPv6 server to a DHCPv6 client.

iana-address prefix *ipv6-address/prefix-length* [**lifetime** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** } }]

No IA_NA address prefix is configured by default.

1.5.4 Configuring the Prefix of a Statically Bound Address to Be Assigned from a DHCPv6 Server to a DHCPv6 Client

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a DHCPv6 address pool and enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure the prefix of a statically bound address to be assigned from a DHCPv6 server to a DHCPv6 client.

prefix-delegation *ipv6-address/prefix-length client*-DUID [**lifetime** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

No static address prefix is configured by default.

1.5.5 Configuring a DCHPv6 Server to Assign Prefixes from a Local Prefix Pool

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a local prefix pool for the PD service of a DHCPv6 server.

ipv6 local pool *pool-name prefix/prefix-length assigned-length*

No local prefix pool is configured for the PD service of a DHCPv6 server by default.

(4) Create a DHCPv6 address pool and enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

(5) Configure the local prefix pool associated with the DHCPv6 server.

prefix-delegation pool *pool-name* [**lifetime** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

No local prefix pool associated with the DHCPv6 server is configured by default.

1.5.6 Configuring Excluded Addresses on a DHCPv6 Server

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a DHCPv6 address pool and enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure excluded addresses on a DHCPv6 server.

excluded-address *start-ipv6-address* [*end-ipv6-address*]

No excluded address is configured on a DHCPv6 server by default.

1.5.7 Enabling the DHCPv6 Server Service

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the DHCPv6 Server service.

ipv6 dhcp server *pool-name* [**rapid-commit**] [**preference** *preference-value*]

The DHCPv6 Server service is disabled by default.

1.6 Configuring the DHCPv6 Server to Assign Other Network Parameters

1.6.1 Overview

A DHCPv6 server can automatically assign configuration parameters, such as the DNS address, domain name, boot file, and Option 52 to DHCPv6 clients.

The DHCPv6 server uses Option 52 to specify the IPv6 address of a Control and Provisioning of Wireless Access Points (CAPWAP) access controller (AC).

1.6.2 Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring the DNS Address to Be Assigned from a DHCPv6 Server to a DHCPv6 Client

- Configuring the Domain Name to Be Assigned from a DHCPv6 Server to a DHCPv6 Client
- Configuring the Boot File URL to Be Assigned from a DHCPv6 Server to a DHCPv6 Client
- Configuring Option 52 on a DHCPv6 Server

1.6.3 Configuring the DNS Address to Be Assigned from a DHCPv6 Server to a DHCPv6 Client

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure the DNS address to be assigned from a DHCPv6 server a DHCPv6 client.

dns-server *ipv6-address*

No DNS address is configured by default.

1.6.4 Configuring the Domain Name to Be Assigned from a DHCPv6 Server to a DHCPv6 Client

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure the domain name to be assigned from a DHCPv6 to a DHCPv6 client.

domain-name *domain*

No domain name is configured by default.

1.6.5 Configuring the Boot File URL to Be Assigned from a DHCPv6 Server to a DHCPv6 Client

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure the boot file Uniform Resource Locator (URL) to be assigned from a DHCPv6 server to a DHCPv6 client.

bootfile-url *url-string*

No boot file URL is configured by default.

1.6.6 Configuring Option 52 on a DHCPv6 Server

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure Option 52 on a DHCPv6 server.

option52 *ipv6-address*

Option 52 is not configured on a DHCPv6 server by default.

1.7 Configuring the DHCPv6 Relay

1.7.1 Overview

A DHCPv6 relay agent can be configured for address assignment, prefix delegation, and parameter allocation between a DHCPv6 client and a DHCPv6 server on different links.

1.7.2 Restrictions and Guidelines

A destination address must be configured for the device with the DHCPv6 relay function enabled. If the destination address is a multicast address (such as FF05::1:3), an egress interface needs to be configured.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the format of **Interface-ID** on a DHCPv6 relay agent.

ipv6 dhcp relay option interface-id format user-defined *text*

The interface name is specified in **Interface-ID** on a DHCPv6 relay agent by default.

(4) (Optional) Configure the format of the MAC address in user-defined options on a DHCPv6 relay agent.

ipv6 dhcp relay option mac-str-format *type*

The default MAC address format is H.H.H.

(5) (Optional) Add **the Remote-ID** to DHCPv6 relay packets.

ipv6 dhcp relay option remote-id enable

DHCPv6 relay packets do not carry **Remote-ID** by default.

(6) (Optional) Configure the format of **Remote-ID** in DHCPv6 relay packets.

ipv6 dhcp relay option remote-id format user-defined *text*

The device DUID is specified for **Remote-ID** in DHCPv6 relay packets by default.

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Enable the DHCPv6 Relay function.

ipv6 dhcp relay destination [**vrf** *vrf-name*] *ipv6-address* [*interface-type interface-number*]

The DHCPv6 Relay function is disabled by default. No destination address or interface over which packets are routed to the destination address is configured.

1.8 Configuring Source Interface Designation Function on a DHCPv6 Relay Agent

1.8.1 Overview

In some device redundancy scenarios, a DHCPv6 server regards uplink interface IP addresses of multiple DHCPv6 relay agents as one IP address. As a result, the DHCPv6 server cannot identify unique DHCPv6 relay agents by their uplink interface IP addresses. The source interface can be designated to differentiate between different DHCPv6 relay agents to ensure normal packet forwarding.

The source interface designation function allows designating an IP address or interface. When a DHCPv6 relay agent forwards a RELAY-FORWARD packet to a DHCPv6 server, specified information is filled in the source IP address and link address fields of the RELAY-FORWARD packet but the destination IP address is still the IP address of the DHCPv6 server. After receiving the RELAY-FORWARD packet, the DHCPv6 server records the source IP address of the packet and uses it as the destination address of the RELAY-REPLY packet. That is, the response packet is destined for the IP address or interface specified by using the source interface designation function of the relay agent, so as to bypass the uplink interface of the DHCPv6 relay agent.

1.8.2 Restrictions and Guidelines

The source interface designation function can be configured in global configuration mode and interface configuration mode. The source interface designation type in interface configuration mode is prior to that in global configuration mode. In one configuration mode, the last configured source interface designation type prevails.

1.8.3 Procedure (Global Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the source interface designation function.

ipv6 dhcp relay source { **source-ip-address** | **gateway-address** } { *ipv6-address* | *interface-type interface-number* }

The source interface designation function is not configured by default.

1.8.4 Procedure (Interface Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface interface-type interface-number

(4) Configure the source interface designation function.

ipv6 dhcp relay source { **source-ip-address** | **gateway-address** } { *ipv6-address* | *interface-type interface-number* }

The source interface designation function is not configured by default.

1.9 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to outputting debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** command to clear information

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear ipv6 dhcp binding [*ipv6-address*]	Clears bindings on a DHCPv6 server.
clear ipv6 dhcp server statistics	Clears statistics of different types of packets on a DHCPv6 server.
clear ipv6 dhcp conflict { *ipv6-address* | * }	Clears conflicted addresses on a DHCPv6 server.

Command	Purpose
clear ipv6 dhcp relay statistics	Clears statistics of different types of packets on a DHCPv6 relay agent.
show ipv6 dhcp	Displays the DUID of a DHCPv6 device.
show ipv6 dhcp binding [*ipv6-address*]	Displays address bindings on a DHCPv6 server.
show ipv6 dhcp interface [*interface-type interface-number*]	Displays interfaces on a DHCPv6 server.
show ipv6 dhcp pool [*pool-name*]	Displays address pools on a DHCPv6 server.
show ipv6 dhcp conflict	Displays conflicted addresses on a DHCPv6 server.
show ipv6 dhcp server statistics	Displays DHCPv6 server statistics.
show ipv6 dhcp relay agent { *ipv6-address* | * }	Displays source interfaces on a DHCPv6 relay agent.
show ipv6 dhcp relay destination { **all** | *interface-type interface-number* }	Displays destination addresses on a DHCPv6 relay agent.
show ipv6 dhcp relay source	Displays the source interface designation configuration on a DHCPv6 relay agent.
show ipv6 dhcp relay statistics	Displays statistics of different types of packets on a DHCPv6 relay agent.
show ipv6 local pool [*pool-name*]	Displays local prefix pool configurations and usage on a device.
debug ipv6 dhcp [**detail**]	Debugs DHCPv6.
debug ipv6 dhcp relay	Debugs a DHCPv6 relay agent.
debug ipv6 dhcp server	Debugs a DHCPv6 server.

1.10 Configuration Examples

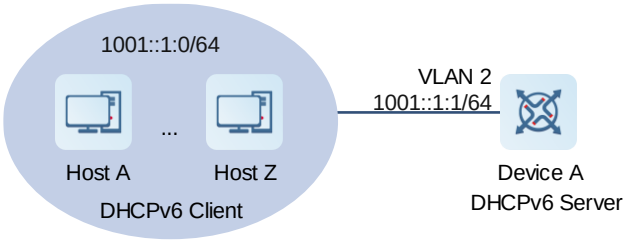
1.10.1 Dynamically Assigning IPv6 Addresses

1. Requirements

As shown in Figure 1-15, a DHCPv6 client in network segment 1001::1:0/64 requests address information from a DHCPv6 server (Device A) in the same subnet. Assignable IPv6 addresses, DNS address, domain name, and other configuration parameters are configured on the DHCPv6 server.

2. Topology

Figure 1-15 Dynamically Assigning IPv6 Addresses



3. Notes

Run the DHCPv6 server on Device A and configure addresses and other parameters for automatic address and parameter assignment.

4. Procedure

(1) Configure Device A:

Configure DHCPv6 address pool parameters.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ipv6 dhcp pool v6
DeviceA(dhcp-config)# iana-address prefix 1001::1:0/64
DeviceA(dhcp-config)# excluded-address 1001::1:1 1001::1:2
DeviceA(dhcp-config)# dns-server 1001::1:2
DeviceA(dhcp-config)# domain-name example.com
```

Configure an interface address and enable the DHCPv6 Server service.

```
DeviceA(config)# interface vlan 2
DeviceA(config-if-VLAN 2)# ipv6 enable
DeviceA(config-if-VLAN 2)# ipv6 address 1001::1:1/64
DeviceA(config-if-VLAN 2)# ipv6 dhcp server v6
```

Cancel suppression of RA messages released on the device.

```
DeviceA(config-if-VLAN 2)# no ipv6 nd suppress-ra
```

Set the configuration flag of managed addresses to **1**, that is, enable hosts to obtain IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 2)# ipv6 nd managed-config-flag
```

Set the configuration flags of other information to **1**, that is, enable hosts to obtain other information except IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 2)# ipv6 nd other-config-flag
```

(2) Configure the hosts:

Enable the dynamic address acquisition function. (Omitted)

5. Verification

Check whether the clients have applied for IPv6 addresses in network segment 1001::1:0/64.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
 ipv6 dhcp pool v6
 iana-address prefix 1001::1:0/64
 excluded-address 1001::1:1 1001::1:2
 dns-server 1001::1:2
 domain-name example.com
!
 interface vlan 2
 ipv6 address 1001::1:1/64
 ipv6 dhcp server v6
!
```

7. Common Errors

- The address pool name exceeds 256 characters.
- The number of configured address pools exceeds 256.
- The number of interfaces configured with the DHCPv6 Server service exceeds 256.
- The number of configured DNS addresses exceeds 10.
- The number of configured domain names exceeds 10.

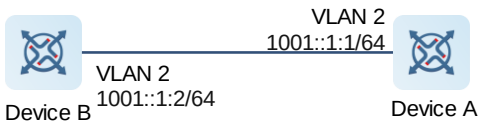
1.10.2 Dynamically Assigning IPv6 Address Prefixes

1. Requirements

As shown in Figure 1-16, Device B is a DHCPv6 client and requests an IPv6 address prefix (2001::1/64), DNS address, domain name, and other network parameters from Device A (a DHCPv6 server).

2. Topology

Figure 1-16 Dynamically Assigning IPv6 Address Prefixes



3. Notes

- Run the DHCPv6 Server service and the PD service on Device A.
- Enable the DHCPv6 Client service on Device B.
- Deploy IPv6 neighbor discovery (ND) between the server and the client to configure host addresses in the subnet through RA messages.

4. Procedure

(1) Configure Device A:

Configure a prefix pool.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)#ipv6 local pool myprefix 2001::1/64 64
```

Configure DHCPv6 address pool parameters and associate it with the prefix pool.

```
DeviceA(config)# ipv6 dhcp pool v6_pd
DeviceA(dhcp-config)# dns-server 1001::1:2
DeviceA(dhcp-config)# domain-name example.com
DeviceA(dhcp-config)# prefix-delegation pool myprefix
DeviceA(dhcp-config)# exit
```

Configure an interface address and enable the DHCPv6 Server service.

```
DeviceA(config)# interface vlan 2
DeviceA(config-if-VLAN 2)# ipv6 enable
DeviceA(config-if-VLAN 2)# ipv6 address 1001::1:1/64
DeviceA(config-if-VLAN 2)# ipv6 dhcp server v6_pd
```

Cancel suppression of RA messages released on the device.

```
DeviceA(config-if-VLAN 2)# no ipv6 nd suppress-ra
```

Set the configuration flag of managed addresses to **1**, that is, enable hosts to obtain IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 2)# ipv6 nd managed-config-flag
```

Set the configuration flags of other information to **1**, that is, enable hosts to obtain other information except IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 2)# ipv6 nd other-config-flag
```

(2) Configure Device B:

Configure an interface address.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface vlan 2
DeviceB(config-if-VLAN 2)# ipv6 enable
DeviceB(config-if-VLAN 2)# ipv6 address 1001::1:2/64
```

Enable the DHCPv6 Client service and request address/prefix information from the DHCPv6 server.

```
DeviceB(config-if-VLAN 2)# ipv6 dhcp client pd mypd
```

5. Verification

Check whether the DHCPv6 Server function is enabled on VLAN 2 of Device A.

```
DeviceA# show ipv6 dhcp interface
VLAN 2 is in server mode
  Server pool: v6_pd
  Rapid-Commit: disable
```

Check whether the DHCPv6 Client function is enabled on VLAN 2 of Device B.

```
DeviceB# show ipv6 dhcp interface
```

```
VLAN 2 is in client mode
  State is IDLE
  next packet will be send in : 43049 seconds
  List of known servers:
    DUID: 00:03:00:01:00:50:56:b0:05:98
    Reachable via address: ::
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x2, T1 43200, T2 69120
        Prefix: 2001::/64
          preferred lifetime 86400, valid lifetime 86400
          expires at Jan 15 2020 16:0 (86249 seconds)
  Prefix name: mypd
  DNS server: 1001::1:2
  Domain name: example.com
  Rapid-Commit: disable
```

Check the common prefix of Device B.

```
DeviceB# show ipv6 general-prefix
There is 1 general prefix.
IPv6 general prefix mypd, acquired via DHCP Prefix Discovery
  2001::/64 valid lifetime 86368, preferred lifetime 86368
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
 ipv6 local pool myprefix 2001::1/64 64
!
 ipv6 dhcp pool v6_pd
 dns-server 1001::1:2
 domain-name example.com
 prefix-delegation pool myprefix
!
 interface vlan 2
 ipv6 address 1001::1:1/64
 ipv6 dhcp server v6_pd
 no ipv6 nd suppress-ra
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
!
```

- Device B configuration file

```
hostname DeviceB
!
 interface vlan 2
 ipv6 address 1001::1:2/64
```

```
 ipv6 dhcp client pd mypd
!
```

7. Common Errors

- The specified address pool name is too long.
- The number of configured address pools exceeds 256.
- The configuration is performed on other interfaces than a SVI, routing port, or L3 AP.
- The number of interfaces configured with the DHCPv6 Server service exceeds 256.
- The number of configured DNS addresses exceeds 10.
- The number of configured domain names exceeds 10.

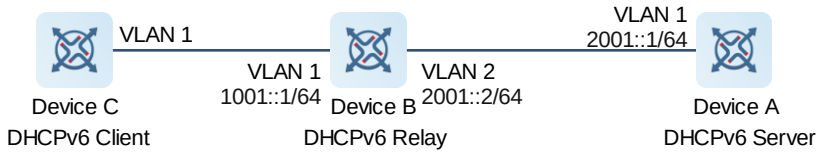
1.10.3 Configuring DHCP Relay

1. Requirements

As shown in Figure 1-17, Device C (a DHCPv6 client) is in network segment 1001::/64, and the address of Device A (a DHCPv6 server) is 2001::1/64. Device B (a DHCPv6 relay agent) provides the relay service for the DHCPv6 client and DHCPv6 server on different links to enable communication between them.

2. Topology

Figure 1-17 Configuring DHCPv6 Relay



3. Notes

- Enable the DHCPv6 Server function on Device A and configure addresses and other parameters.
- Enable the DHCPv6 Relay function on Device B with the destination address pointed to VLAN 1 on Device A.
- Enable the DHCPv6 Client function on Device C.

4. Procedure

(1) Configure Device A:

Configure DHCPv6 address pool parameters.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ipv6 dhcp pool v6
DeviceA(dhcp-config)# iana-address prefix 1001::/64
DeviceA(dhcp-config)# excluded-address 1001::1 1001::2
DeviceA(dhcp-config)# dns-server 1001::2
DeviceA(dhcp-config)# domain-name example.com
```

Configure an interface address and enable the DHCPv6 Server service.

```
DeviceA(config)# interface vlan 1
DeviceA(config-if-VLAN 1)# ipv6 enable
DeviceA(config-if-VLAN 1)# ipv6 address 2001::1/64
DeviceA(config-if-VLAN 1)# ipv6 dhcp server v6
```

Cancel suppression of RA messages released on the device.

```
DeviceA(config-if-VLAN 1)# no ipv6 nd suppress-ra
```

Set the configuration flag of managed addresses to **1**, that is, enable hosts to obtain IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 1)# ipv6 nd managed-config-flag
```

Set the configuration flags of other information to **1**, that is, enable hosts to obtain other information except IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 1)# ipv6 nd other-config-flag
```

(2) Configure Device B:

Configure an uplink interface address.

```
DeviceB> enable
DeviceB#configure terminal
DeviceB(config)# interface vlan 2
DeviceB(config-if-VLAN 2)# ipv6 enable
DeviceB(config-if-VLAN 2)# ipv6 address 2001::2/64
DeviceB(config-if-VLAN 2)# exit
```

Configure a downlink interface address and enable the DHCPv6 Relay function.

```
DeviceB(config)#interface vlan 1
DeviceB(config-if-VLAN 1)# ipv6 enable
DeviceB(config-if-VLAN 1)# ipv6 address 1001::1/64
DeviceB(config-if-VLAN 1)# ipv6 dhcp relay destination 2001::2
```

(3) Configure Device C:

Enable the DHCPv6 Client function to apply for an IP address.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)#interface vlan 1
DeviceC(config-if-VLAN 1)#ipv6 dhcp client ia
```

5. Verification

Check whether Device C has applied for an IPv6 address in network segment 1001::/64.

```
DeviceC# show ipv6 interface

interface VLAN 1 is Up, ifindex: 2, vrf_id 0
  address(es):
    Mac Address: 00:50:56:b0:2f:50
    INET6: 1001::3 [ TENTATIVE ], subnet is 1001::/64
      valid lifetime 86400 sec, preferred lifetime 86400 sec
  Joined group address(es):
```

```
  FF01::1
  FF02::1
  FF02::2
  FF02::1:FF00:0
  FF02::1:FF00:3
  FF02::1:FFB0:2F50
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND stale time is 3600 seconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 600 seconds<480--720>
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
 ipv6 dhcp pool v6
 iana-address prefix 1001::/64
 excluded-address 1001::1 1001::2
 dns-server 1001::2
 domain-name example.com
!
 interface vlan 1
 ipv6 address 2001::1/64
 ipv6 dhcp server v6
 no ipv6 nd suppress-ra
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
!
```

- Device B configuration file

```
hostname DeviceB
!
 interface vlan 2
 ipv6 enable
 ipv6 address 2001::2/64
!
 interface vlan 1
 ipv6 address 1001::1/64
```

```
 ipv6 dhcp relay destination 2001::2
!
```

- Device C configuration file

```
hostname DeviceC
!
 interface vlan 1
 ipv6 dhcp client ia
!
```

Contents

1 Configuring DHCPv6 Client 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 1
1.2 Restrictions and Guidelines 1
1.3 Configuring DHCPv6 Client to Request an IPv6 Address 1
1.3.1 Overview 1
1.3.2 Restrictions and Guidelines 2
1.3.3 Procedure 2
1.4 Configuring DHCPv6 Client to Request an IPv6 Prefix 2
1.4.1 Overview 2
1.4.2 Restrictions and Guidelines 2
1.4.3 Procedure 2
1.5 Monitoring 3

1 Configuring DHCPv6 Client

1.1 Introduction

1.1.1 Overview

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is used to assign IPv6 addresses, IPv6 prefixes, and other network configuration parameters to client hosts.

When a device serves as a DHCPv6 client, the device can:

- Obtain an IPv6 address and network configuration parameters by using DHCPv6. The IPv6 address is used as the address of an interface on which the DHCPv6 Client function is enabled.
- Obtain an IPv6 prefix and network configuration parameters by using DHCPv6. The IPv6 prefix is used by the device to generate an IPv6 address.
- Obtain an IPv6 address, IPv6 prefix, and network configuration parameters by using DHCPv6. The IPv6 address is used as the address of an interface on which the DHCPv6 Client function is enabled, and the IPv6 prefix is used by the device to generate an IPv6 address.
- Obtain network configuration parameters except the IPv6 address and prefix through DHCPv6 stateless configuration.

1.1.2 Principles

DHCPv6 is a protocol based on the client/server model. For details about interaction between a DHCPv6 client and a DHCPv6 server, see "Configuring DHCPv6."

1.1.3 Protocols and Standards

- RFC 3315: Dynamic Host Configuration Protocol for IPv6
- RFC 3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6
- RFC 3646: DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3736: Stateless DHCP Service for IPv6
- RFC 5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

1.2 Restrictions and Guidelines

You are advised not to enable both the DHCPv6 Client and DHCPv6 Server functions or both the DHCPv6 Client and DHCPv6 Relay functions on the same interface. Otherwise, the functions may be abnormal.

1.3 Configuring DHCPv6 Client to Request an IPv6 Address

1.3.1 Overview

Configure a device as a DHCPv6 client to automatically request an IPv6 address or related parameters from a DHCPv6 server.

1.3.2 Restrictions and Guidelines

The DHCPv6 Client function can be configured only on L3 interfaces.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the DHCPv6 Client function and request an identity association non-temporary address (IA_NA) address.

ipv6 dhcp client ia [**rapid-commit**]

IA_NA address requesting is disabled by default.

(5) (Optional) Configure the stateless service.

ipv6 nd other-config-flag

The stateless service is not configured by default.

1.4 Configuring DHCPv6 Client to Request an IPv6 Prefix

1.4.1 Overview

Configure a device as a DHCPv6 client to automatically request an IPv6 prefix or related parameters from a DHCPv6 server.

1.4.2 Restrictions and Guidelines

The DHCPv6 Client function can be configured only on L3 interfaces.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the DHCPv6 Client function to request an IPv6 prefix.

ipv6 dhcp client pd *prefix-name* [**rapid-commit**]

Address prefix requesting is not configured by default.

1.5 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to outputting debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** command to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear ipv6 dhcp client *interface-type interface-number*	Restarts the DHCPv6 Client function.
show ipv6 dhcp	Displays the DHCP Unique Identifier (DUID) of a device.
show ipv6 dhcp interface [*interface-type interface-number*]	Displays DHCPv6 interfaces.
debug ipv6 dhcp [**detail**]	Debugs DHCPv6.
debug ipv6 dhcp client	Debugs a DHCPv6 client.

Contents

1 Configuring DHCPv6 Snooping 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Applications 6
1.1.4 Protocols and Standards 8
1.2 Restrictions and Guidelines 8
1.3 Configuration Task Summary 9
1.4 Configuring Basic DHCPv6 Snooping Functions 9
1.4.1 Overview 9
1.4.2 Procedure 9
1.5 Configuring Optional DHCPv6 Snooping Functions 9
1.6 Configuring Option 18 or 37 10
1.7 Monitoring 10
1.8 Configuration Examples 12
1.8.1 Configuring Basic DHCPv6 Snooping Functions 12
1.9 Common Misconfigurations 13

1 Configuring DHCPv6 Snooping

1.1 Introduction

1.1.1 Overview

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) snooping snoops DHCPv6 packets are exchanged between clients and servers, including request packets from the clients and response packets from the servers. These packets are used to record and monitor usage of IPv6 addresses and filter out invalid DHCPv6 packets. User data entries generated from DHCPv6 snooping records may serve security applications such as IPv6 Source Guard.

1.1.2 Principles

1. Basic Concepts

- DHCPv6 request packets

  Request packets are sent from a DHCPv6 client to a DHCPv6 server, including DHCPv6 SOLICIT, DHCPv6 REQUEST, DHCPv6 CONFIRM, DHCPv6 REBIND, DHCPv6 RELEASE, DHCPv6 DECLINE, DHCPv6 RENEW, DHCPv6 INFORM_REQ, and DHCPv6 LEASEQUERY packets.

- DHCPv6 response packets

  Response packets are sent from a DHCPv6 server to a DHCPv6 client, including DHCPv6 ADVERTISE, DHCPv6 REPLY, DHCPv6 RECONFIGURE, DHCPv6 RELAY_REPLY, DHCPv6 LEASEQUERY_REPLY, DHCPv6 LEASEQUERY_DONE, and DHCPv6 LEASEQUERY_DATA packets.

- VLAN-based DHCPv6 Snooping

  DHCPv6 Snooping is enabled on a per-VLAN basis. When DHCPv6 Snooping is enabled, it is effective to all virtual local area networks (VLANs) on the current device by default. You can flexibly specify the VLANs to which DHCPv6 Snooping takes effect.

- DHCPv6 Snooping trusted ports

  Packets for obtaining IPv6 addresses or prefixes through DHCPv6 are exchanged via multicast. Rogue DHCPv6 services may affect normal acquisition of IPv6 addresses and lead to spoofing and stealing of user information. To prevent rogue DHCPv6 services, DHCPv6 Snooping ports are classified into two types: trusted and untrusted.

  A device with DHCPv6 Snooping enabled only transmits DHCPv6 response packets received on trusted ports and discards those from untrusted ones. In this way, the ports connected to legitimate DHCP servers are configured as trusted ports and the other ports are configured as untrusted ports to shield rough DHCPv6 servers.

  On switches, all switching ports or L2 aggregation ports (APs) are defaulted as untrusted, and trusted ports can be specified.

- DHCPv6 Snooping binding database

  In a DHCPv6 network, clients may set static IPv6 addresses randomly. This increases not only the difficulty of network maintenance but also the possibility that legitimate clients with IPv6 addresses assigned by a

DHCPv6 server may fail to use the network due to address conflicts. By snooping packets between the clients and servers, DHCPv6 Snooping summarizes user entries, including IPv6 addresses, Media Access Control (MAC) addresses, VLAN IDs (VIDs), ports, and lease time to build the DHCPv6 Snooping binding database, ensuring proper use of IPv6 addresses.

- DHCPv6 Snooping packet suppression

  To shield all the DHCPv6 packets on a specific client, enable DHCPv6 Snooping packet suppression on untrusted ports.

- Invalid DHCPv6 packets

  The device with DHCPv6 Snooping enabled check validity of received DHCPv6 packets, discards invalid DHCPv6 packets, and records information about legitimate users to form the DHCPv6 Snooping binding database for query by other applications. The following types of packets are considered as invalid DHCPv6 packets:

  - DHCPv6 response packets received on untrusted ports. For details, see description about DHCPv6 response packets in "Basic Concepts".
  - Relayed DHCPv6 packets received on untrusted ports, that is, the DHCPv6 RELAY_FORW and DHCPv6 RELAY_REPLY packets
  - DHCPv6 RELAY_REPLY packets received on trusted ports with untrusted outbound ports
  - DHCPv6_RELEASE packets with no entries in the DHCPv6 Snooping binding database found based on the source MAC addresses and VIDs in the packets
  - DHCPv6_RELEASE packets that carry IPv6 addresses or prefixes that are not existed in the DHCPv6 Snooping binding database
  - DHCPv6_RELEASE packets that carry IPv6 addresses or prefixes existing in the DHCPv6 Snooping binding database but having untrusted ports unmatched with those saved in the DHCPv6 Snooping binding database
  - DHCPv6 packets in invalid formats or incomplete DHCPv6 packets

2. Building a DHCPv6 Snooping Binding Database

The device with DHCPv6 Snooping enabled detects packets exchanged between DHCPv6 clients and DHCPv6 servers and generates entries in the DHCPv6 Snooping binding database and prefix database based on information of valid DHCPv6 packets. All these entries are used as the information table of legitimate users, and provided to other security modules of the device as the basis for filtering network packets.

The binding database and prefix database are updated during snooping based on the types of DHCPv6 packets.

- Generating binding or prefix entries

  When a DHCPv6 REPLY packet is snooped on a trusted port, the device with DHCPv6 Snooping enabled extracts the client's IPv6 address or prefix, MAC address, and lease time from the packet and generates a binding or prefix entry based on the client's port ID (interface index) and VLAN ID that are recorded on the device.

- Deleting binding or prefix entries

  A binding or prefix entry is deleted in the following scenarios:

  - The recorded lease time expires.

- A valid DHCPv6 RELEASE or DHCPv6 DECLINE packet from a client is snooped.
- A client user runs the **clear** command to delete a binding or prefix entry.

3. DHCPv6 Option 18 or 37

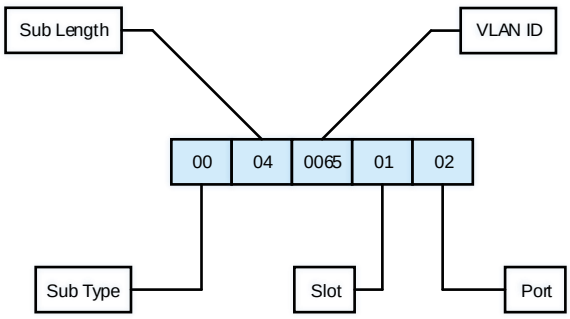
Some network administrators want to assign and manage IP addresses based on information about the network devices connected user clients (that is, client locations). To meet this requirement, a device with DHCPv6 Snooping enabled adds related network device information to DHCPv6 request packets by using a DHCPv6 option, which is Option 18 in RFC 3315 and Option 37 in RFC 4649. After Option 18 or 37 parsing is configured on a DHCPv6 server, the DHCPv6 server can obtain more user information based on the content of Option 18 or 37 and assign IP addresses to users more accurately.

- Option 18: Interface ID

  The default padding content of **Interface ID** is the ID of the VLAN to which the port receiving DHCPv6 request packets from clients resides or the index of the port. The port index value is the corresponding slot ID and port number. The extended padding content is a user-defined string. Extended padding is valid only to wired ports by default. Wired ports include switching ports, L2 APs, and L2 encapsulation sub-interfaces. For wireless ports, the extended padding content is **0**.

  Interface ID supports two padding formats: standard padding and extended padding. In a network, only one padding format can be used. In standard padding format, only the default padding content of is padded, as shown in the following figure.

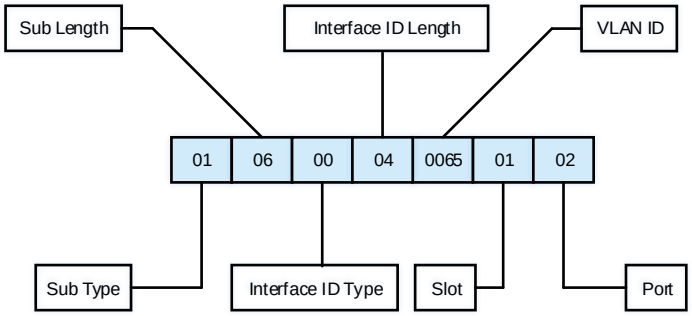
Figure 1-1 Standard Padding Format of Interface ID



If user-defined padding content is required, use the extended padding format. In extended padding format, the padding content can be the default padding content or extended padding content. To distinguish between different padding content, a 1-byte content type field and a 1-byte content length field are added after the sub-option length field. For default padding content, the content type is set to **0**. For extended padding content, the content type is set to **1**.

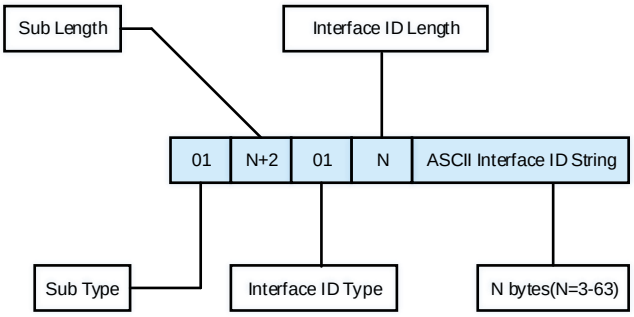
The following figure shows the default padding content in extended padding format.

Figure 1-2 Default Padding Content of Interface ID in Extended Padding Format



The following figure shows the extended padding content in extended padding format.

Figure 1-3 Extended Padding Content of Interface ID in Extended Padding Format

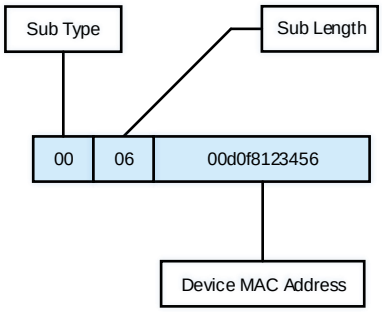


- Option 37: Remote ID

  The default padding content of **Remote ID** is the MAC address of the DHCPv6 relay that receives request packets from DHCPv6 clients, and the extended padding content is a user-defined string.

  Remote ID supports two padding formats: standard padding and extended padding. In a network, only one padding format can be used. In standard padding format, only the default padding content is padded, as shown in the following figure.

Figure 1-4 Standard Padding Format of Remote ID

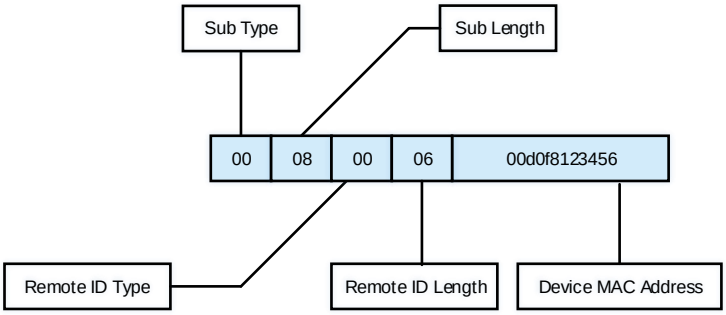


If user-defined padding content is required, use the extended padding format. In extended padding format, the padding content can be the default padding content or extended padding content. To distinguish between different padding content, a 1-byte content type field and a 1-byte content length field are added

after the sub-option length field. For default padding content, the content type is set to **0**. For extended padding content, the content type is set to **1**.

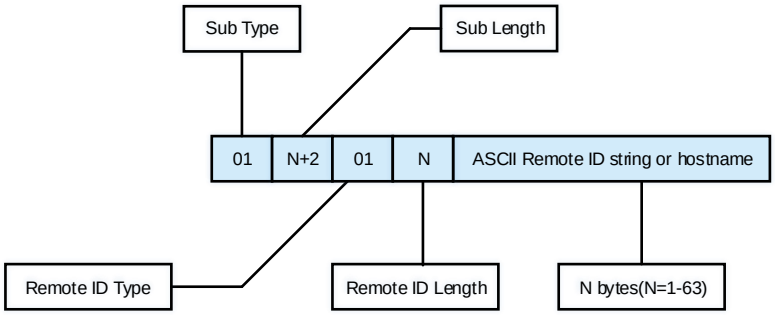
The following figure shows the default padding content in extended padding format.

Figure 1-5 Default Padding Content of Remote ID in Extended Padding Format



The following figure shows the extended padding content in extended padding format.

Figure 1-6 Extended Padding Content of Remote ID in Extended Padding Format



In **Interface ID** of Option 18, the port index value is the slot ID and port number. The port can be a switching port, L2 AP, or L2 encapsulation sub-interface. The port number indicates the serial number (SN) of a port in a slot. The port number of an L2 AP is the AP number. For example, if the switching port name is Fa0/10, the port number is 10. If the AP name is AP 11, the port number is 11. If the WLAN port name is WLAN 1, the port number is 1.

The slot ID is the SN of a slot on a device (stacked devices are regarded as one). The slot ID of an AP is placed at the end. Slot IDs are numbered starting from 0. You can run the **show slots** command to display slot IDs. For example:

```
Ruijie# show slots
  Dev Slot
  --- ----
  1   0    ------> The slot ID is 0.
  1   1    ------> The slot ID is 1.
  1   2    ------> The slot ID is 2.
```

In this case, the slot ID of the AP is 3.

```
Ruijie# show slots
```

```
Dev Slot
--- ----
1   0    ------> The slot ID is 0.
1   1    ------> The slot ID is 1.
1   2    ------> The slot ID is 2.
2   0    ------> The slot ID is 3.
2   1    ------> The slot ID is 4.
2   2    ------> The slot ID is 5.
```

In this case, the slot ID of the AP is 6.

1.1.3 Applications

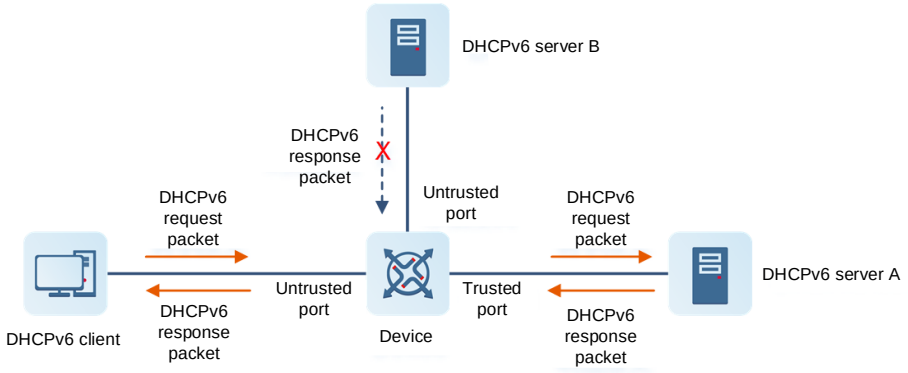
1. Guarding Against DHCPv6 Spoofing

Multiple DHCPv6 servers may exist in a network. It is essential to ensure that user PCs obtain network configurations only from the DHCP servers within a controlled area.

As shown in the following figure, the DHCPv6 client can communicate only with trusted DHCPv6 servers.

- Request packets from the DHCPv6 client are transmitted only to trusted DHCPv6 servers.
- Only response packets from trusted DHCPv6 servers can be transmitted to the DHCPv6 client.

Figure 1-7 Guarding Against DHCPv6 Spoofing



Device is an access device, DHCPv6 Server A is in the controlled area, and DHCPv6 Server B is beyond the controlled area.

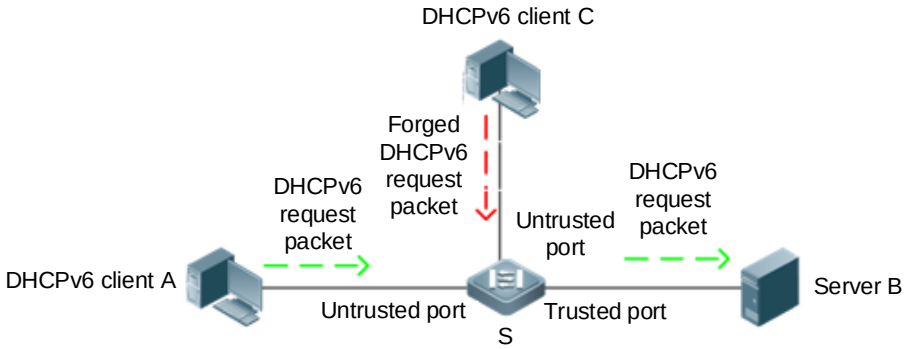
- DHCPv6 Snooping is enabled on Device to monitor DHCPv6 packets.
- The port on Device for connecting to DHCPv6 Server A is configured as a DHCPv6 trusted port to forward response packets.
- The rest ports on Device are configured as DHCPv6 untrusted ports to filter response packets.

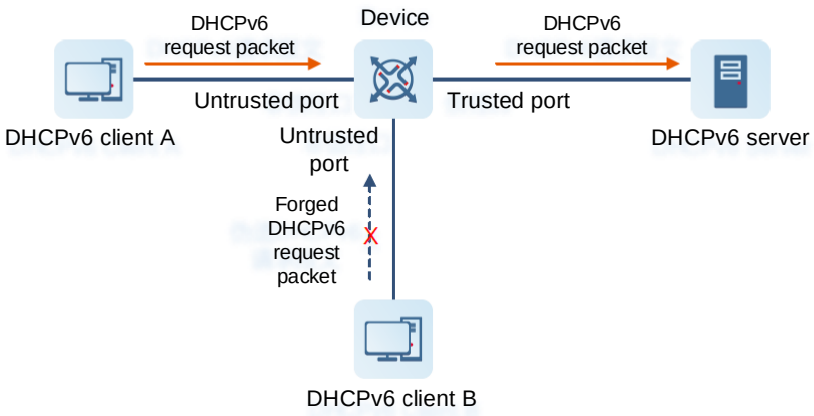
2. Guarding Against Forged DHCPv6 Packets

Malicious DHCPv6 clients in a network may forge DHCPv6 request packets, which consumes applicable IPv6 addresses from the servers and probably preempts legitimate users' IPv6 addresses. Therefore, it is necessary to filter out invalid DHCPv6 packets.

As shown in the following figure, request packets sent from a DHCPv6 client are checked. The RELEASE and DECLINE packets from clients must match the entries in the DHCPv6 Snooping binding database.

Figure 1-8 Guarding Against Forged DHCPv6 Packets





Device is an access device, and DHCPv6 Server is in the controlled area.

- DHCPv6 Snooping is enabled on Device to monitor DHCPv6 packets.
- The port on Device for connecting to DHCPv6 Server is configured as a DHCPv6 trusted port to forward response packets.
- The rest ports on Device are configured as DHCPv6 untrusted ports to filter DHCPv6 packets.

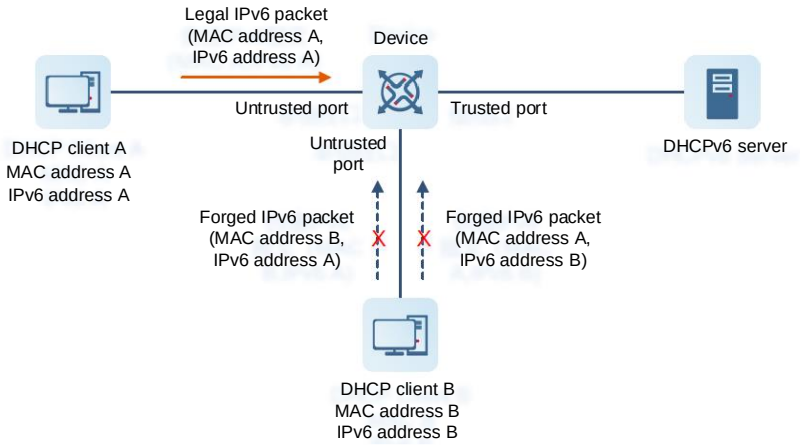
3. Guarding Against IPv6/MAC Address Spoofing

You can check IPv6 packets from untrusted ports based on the IP address field or IP address and MAC address fields to filter out forged IPv6 packets.

As shown in the following figure, IPv6 packets sent from a DHCPv6 client are checked.

- The source address fields in IPv6 packets must match IPv6 addresses assigned by the DHCPv6 server.
- The source MAC address field in L2 packets must match the client MAC address field in DHCPv6 request packets from clients.

Figure 1-9 Guarding Against IPv6/MAC Address Spoofing



Device is an access device, and DHCPv6 Server is in the controlled area.

- DHCPv6 Snooping is enabled on Device to monitor DHCPv6 packets.
- The port on Device for connecting to DHCPv6 Server is configured as a DHCPv6 trusted port.
- The rest ports on Device are configured as DHCPv6 untrusted ports.
- IPv6 Source Guard is enabled on Device to filter IPv6 packets.
- The IPv6 Source Guard matching mode is set to IP+MAC on Device to check the MAC address and IPv6 address fields in IPv6 packets.

4. Preventing Private IPv6 Addresses

The device with DHCPv6 Snooping enabled checks whether the source IPv6 addresses in IPv6 packets from untrusted ports are consistent with the addresses assigned by the DHCPv6 server.

If the source IPv6 addresses, connected ports, and L2 source MAC addresses in IPv6 packets do not match the assignments of the DHCPv6 server, such packets are discarded.

The working process of the device in this scenario is the same as that in "Guarding Against IPv6/MAC Address Spoofing."

1.1.4 Protocols and Standards

- RFC 3315: Dynamic Host Configuration Protocol For IPv6
- RFC 5007: DHCPv6 Leasequery
- RFC 5460: DHCPv6 Bulk Leasequery

1.2 Restrictions and Guidelines

- The ports on clients for connecting to trusted DHCPv6 servers must be configured as DHCPv6 trusted ports.
- DHCPv6 Snooping takes effect on switching ports, L2 APs, and L2 encapsulation sub-interfaces.
- The function of clearing entries of linkdown ports takes effect only to wired ports.

1.3 Configuration Task Summary

DHCPv6 Snooping configuration includes the following tasks:

(1) Configuring Basic DHCPv6 Snooping Functions

(2) Configuring Optional DHCPv6 Snooping Functions

(3) (Optional) Configuring Option 18 or 37

1.4 Configuring Basic DHCPv6 Snooping Functions

1.4.1 Overview

Enable basic DHCPv6 Snooping functions to filter out invalid DHCPv6 packets and control the transmission scope of DHCPv6 packets.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCPv6 Snooping globally.

ipv6 dhcp snooping

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure an interface as a DHCPv6 Snooping trusted port.

ipv6 dhcp snooping trust

All interfaces are DHCPv6 Snooping untrusted ports by default.

1.5 Configuring Optional DHCPv6 Snooping Functions

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure optional DHCPv6 Snooping functions. Perform at least one of the following configuration steps:

- Disable DHCPv6 Snooping on a VLAN.

  no ipv6 dhcp snooping vlan { *vlan-range* | *vlan-min* [*vlan-max*] }

  After DHCPv6 Snooping is enabled globally, it takes effect to all VLANs by default.

- Write all dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time.

  ipv6 dhcp snooping database write-delay *time*

The function of writing all dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time is not configured by default.

- Configure an interface to filter all DHCPv6 request packets. Run the following commands in turn.

  interface *interface-type interface-number*

  ipv6 dhcp snooping filter-dhcp-pkt

  No interface is configured to filter all DHCPv6 request packets by default.

1.6 Configuring Option 18 or 37

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Add Option 18 or 37 to DHCPv6 request packets.

ipv6 dhcp snooping information option [**standard-format**]

Option 18 or 37 is not added to DHCPv6 request packets by default.

(4) (Optional) Set **Remote ID** to a user-defined string or the host name when Option 37 is in extended padding mode.

ipv6 dhcp snooping information option format remote-id { **hostname** | **string** *ascii-string* }

When Option 37 is in extended padding mode, **Remote ID** is not set to a user-defined string or host name by default.

(5) Enter the interface configuration mode.

interface *interface-type interface-number*

(6) (Optional) Set **Interface ID** to a user-defined string when Option 18 is in extended padding mode.

ipv6 dhcp snooping vlan *vlan-id* **information option format-type interface-id string** *ascii-string*

Interface ID is not set to a user-defined string by default when Option 18 is in extended padding mode.

(7) (Optional) Change the padded VLAN to a specified VLAN when Option 18 is in extended padding mode.

ipv6 dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

When Option 18 is in extended padding mode, the padded VLAN is not changed to a specified VLAN by default.

1.7 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the clear command to clear information.

Run the **debug** command to output debugging information.

Caution

- Running the **clear** commands may lose vital information and thus interrupt services.
- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
show ipv6 dhcp snooping	Displays DHCPv6 Snooping configurations.
show ipv6 dhcp snooping vlan	Displays VLANs to which DHCPv6 Snooping does not take effect.
show ipv6 dhcp snooping binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Displays dynamic user information in the DHCPv6 Snooping binding database.
show ipv6 dhcp snooping prefix [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Displays user information in the DHCPv6 Snooping prefix database.
show ipv6 dhcp snooping statistics	Displays DHCPv6 Snooping packet statistics.
show ipv6 dhcp snooping packet	Displays DHCPv6 Snooping packet statistics on an interface.
clear ipv6 dhcp snooping binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Clears dynamic user information in the DHCPv6 Snooping binding database.
clear ipv6 dhcp snooping prefix [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Clears all entries in the DHCPv6 Snooping prefix database.
clear ipv6 dhcp snooping statistics	Clears DHCPv6 Snooping packet statistics.
debug snooping ipv6 event	Debugs DHCPv6 Snooping events.
no debug snooping ipv6 event	Disables debugging of DHCPv6 Snooping events.
debug snooping ipv6 packet	Debugs DHCPv6 Snooping packets.
no debug snooping ipv6 packet	Disables debugging of DHCPv6 Snooping packets.

1.8 Configuration Examples

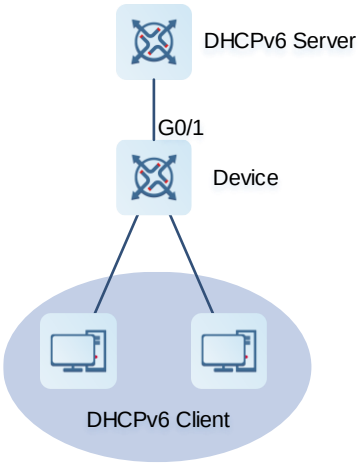
1.8.1 Configuring Basic DHCPv6 Snooping Functions

1. Requirements

DHCPv6 clients can obtain IPv6 addresses from legitimate DHCPv6 servers dynamically.

2. Topology

Figure 1-10 Topology of Configuring Basic DHCPv6 Snooping Functions



3. Notes

- Enable DHCPv6 Snooping on Device (an access device).
- Configure the uplink interface GigabitEthernet 0/1 as a trusted port.

4. Procedure

Enable DHCPv6 Snooping on Device.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp snooping
Device(config)# interface gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ipv6 dhcp snooping trust
```

5. Verification

Display DHCPv6 Snooping configurations on Device and check whether the trusted port is correct.

```
Device# show ipv6 dhcp snooping
DHCPv6 snooping status                  : ENABLE
DHCPv6 snooping database write-delay time : 0 seconds
DHCPv6 snooping binding-delay time       : 0 seconds
DHCPv6 snooping option18/37 status       : DISABLE
DHCPv6 snooping link detection           : DISABLE
Interface                Trusted    Filter DHCPv6
```

```
------------------------   -------   -------------
GigabitEthernet 0/1        YES       DISABLE
```

Display entries generated by Device.

```
Device# show ipv6 dhcp snooping binding
Total number of bindings: 1
NO.   MAC Address        IPv6 Address                            Lease(sec)   VLAN
Interface
1    00d0.f801.0101     2001::10                               42368       2
GigabitEthernet 0/1
```

6. Configuration Files

Device configuration file

```
hostname Device
!
ipv6 dhcp snooping
!
interface GigabitEthernet 0/1
 ipv6 dhcp snooping trust
!
end
```

1.9 Common Misconfigurations

- The uplink interface is not configured as a DHCPv6 Snooping trusted port.
- Another access security option is configured for the uplink interface. As a result, the uplink interface fails to be configured as a DHCPv6 Snooping trusted port.

Contents

1 Configuring ND Snooping 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 4
1.2 Configuration Task Summary 4
1.3 Configuring Basic ND Snooping Functions 5
1.4 Configuring ND Guard 5
1.5 Configuring ND Logging 6
1.6 Monitoring 7
1.7 Configuration Examples 7
1.7.1 Configuring ND Guard 7

1 Configuring ND Snooping

1.1 Introduction

1.1.1 Overview

The Neighbor Discovery Protocol (NDP) is susceptible to address spoofing and routing information attacks due to its deficiency in inherent security. However, it is complex to enhance security by deploying an external encryption and authentication system. ND Snooping is used to monitor ND packets in a network to filter out invalid address resolution packets and RA packets, monitor IPv6 users in the network, and bind detected IPv6 users to interfaces to prevent IP address spoofing and build a secure and trusted IPv6 network.

1.1.2 Principles

1. NDP

NDP is a core protocol of the IPv6 suite. It combines and optimizes protocols such as the Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) Router Discovery, and ICMP Redirect in IPv4. As a basic IPv6 protocol, NDP also provides the prefix discovery, neighbor unreachability detection (NUD), duplicate address detection (DAD), and auto address configuration functions.

- Address resolution: a method to determine the link-layer address (LLA) of a target node. The address resolution function of NDP replaces ARP in IPv4 and uses the NUD method to maintain the reachability status between neighbors.
- Stateless Address Autoconfiguration (SLACC): unique SLACC mechanism in NDP, including a series of related functions, such as router discovery, automatic interface ID generation, and DAD. Through SLACC, nodes on a link can automatically obtain global unicast IPv6 addresses.
- Redirection: When a better router for reaching the destination network is found on the local link, the original router needs to send advertisements to nodes, for the nodes to change related configurations.

2. ND Snooping Entries

- Entry creation mechanism

  When receiving an ND packet from an unknown source address, the device creates an ND Snooping entry in **TENTATIVE** state. Then, the device sends a specified number of DAD neighbor solicitation (NS) packets to ND Snooping trusted ports (ports configured with the **ipv6 nd snooping trust** command) for snooping. The number of packets to be sent and the sending interval are configured by running the **ipv6 nd snooping detect packet** command. If no neighbor advertisement (NA) response is received within the **TENTATIVE** state timeout time (which can be configured by running the **ipv6 nd snooping tentative wait** command) after the last NS packet is sent, no conflicted addresses exist in the local area network (LAN). The ND Snooping entry is changed to the **VALID** state. If an NA packet is received within the **TENTATIVE** state timeout time after an NS packet is sent, conflicted addresses exist in the LAN. In this case, the device deletes the ND Snooping entry.
- Entry migration mechanism

  Entry migration includes the following types:

- Intra-device migration

  When the device receives an ND packet with the same source address as an existing ND Snooping entry from an ND Snooping untrusted port in the same VLAN, the entry state is changed to **TESTING_VP**. Then, the device sends a specified number of DAD NS packets to the inbound port that learns the ND Snooping entry for snooping. The number of packets to be sent and the sending interval are configured by running the **ipv6 nd snooping detect packet** command. If no NA packet is received within the **TESTING_VP** state timeout time (which can be configured by running the **ipv6 nd snooping detect wait** command), the original user is disconnected from the inbound port. The device changes the inbound port of the ND Snooping entry to the port receiving the new packet and changes the entry state to **VALID**. If an NA packet is received within the **TESTING_VP** state timeout time after the first NS packet is sent, the inbound port of the ND Snooping entry remains unchanged and the entry state is restored to **VALID**.

- Inter-device migration

  When the device receives an ND packet with the same source address as an existing ND snooping entry from an ND Snooping trusted port, the ND Snooping entry is changed to the **TESTING_TP-LT** state. Then, the device sends a specified number of DAD NS packets to the inbound port that learns the ND Snooping entry for snooping. The number of packets to be sent and the sending interval are configured by running the **ipv6 nd snooping detect packet** command. If no NA packet is received within the **TESTING_TP-LT** state timeout time (which can be configured by running the **ipv6 nd snooping detect wait** command), the original user is disconnected from the inbound port. Then, the device deletes the corresponding ND Snooping entry, and the device connected to the ND trusted port creates an ND Snooping entry. In this case, cross-device entry migration is complete. If an NA packet is received within the **TESTING_TP-LT** state timeout time after the NS packets are sent, the original user is not disconnected from the inbound port. In this case, the device reserves the corresponding ND Snooping entry, changes the entry state to **VALID**, and forwards the NA packet to the trusted port.

- Entry aging mechanism

  If no ND packet is received within the **VALID** state timeout time (which can be configured by running the **ipv6 nd snooping bind lifetime** command) since the last update of an ND Snooping entry, the ND Snooping entry is changed to the **TESTING_TP-LT** state. Then, the device sends a specified number of DAD NS packets to the inbound port that learns the ND Snooping entry for snooping. The number of packets to be sent and the sending interval are configured by running the **ipv6 nd snooping detect packet** command. If no NA packet is received within the **TESTING_TP-LT** state timeout time (which can be configured by running the **ipv6 nd snooping detect wait** command), the original user is disconnected from the inbound port. The device deletes the ND Snooping entry. If an NA packet is received within the **TESTING_TP-LT** state timeout time, the original user is not disconnected from the inbound port. In this case, the device reserves the ND Snooping entry, changes the entry state to **VALID**, and resets the timeout time.

3. ND Snooping

ND Snooping supports the following functions:

- ND guard

  When SLACC is used, IPv6 nodes use RA information to configure interface IPv6 addresses and obtain the prefixes of direct-connected network segments, gateway IP addresses, and maximum transmission units

(MTUs) of links. In addition, routers can use ND redirect packets to modify the next-hop information of related routes in the routing tables of hosts. In this case, attackers can send invalid RA and redirect packets and modify routing table information (such as the gateway IP address) of the attacked host to initiate denial-of-service (DoS) and man-in-the-middle (MITM) attacks. This type of attacks for spoofing hosts' routing information is called routing information attacks.

During unicast communication between IPv6 nodes, the NDP is used for address resolution to obtain LLAs of neighboring nodes. Then, the parsed LLAs are encapsulated into frames to be sent. Five types of ND packets can carry the LLA, and the receiving nodes regard the packets as trusted. Therefore, attackers can send forged ND packets and modify the mappings between IP addresses and LLAs in the neighbor table of the attacked node to initiate DoS and MITM attacks. This type of attacks for spoofing the mappings between IP addresses and LLAs on nodes is called ARP attacks.

To prevent the preceding two types of attacks, ND Snooping classifies interfaces on network devices into trusted interfaces and untrusted interfaces. Trusted interfaces are used to connect trusted nodes, such as the routers and servers, and untrusted interfaces are used to connect untrusted nodes, such as PCs. The device forwards ND packets received on trusted interfaces and discards redirect and RA packets received on untrusted interfaces to prevent routing information attacks. For router solicitation (RS), NS, and NA packets received on untrusted interfaces, the device checks the packet validity and discards invalid ones to prevent address spoofing attacks.

For NS and NA packets, the device checks mappings of the source IP address, destination IP address, VLAN ID (VID), Media Access Control (MAC) address, and inbound interface. The mappings of the four elements of host nodes are provided by monitoring SLACC users. If an NA packet received on an untrusted interface carries information that can be set only by a router (R bit is set to 1), the packet is regarded as invalid.

Security check on ND packets from all host nodes prevent gateway address spoofing attacks. To guard against only gateway address spoofing attack address spoofing attacks, see "ND guard against gateway address spoofing attacks." ND guard against RA attacks is regardless of the preceding factors. You can enable ND guard against address spoofing attacks by running the corresponding command. ND guard against RA attacks is enabled when ND snooping is enabled.

- ND guard against gateway address spoofing attacks

  Gateway address spoofing is a common attack method and causes severe adverse impact. If gateway address spoofing attacks are eliminated, a network is free from most address spoofing attacks. In addition, when only ND guard against gateway address spoofing attacks is enabled, system resources are saved. To facilitate use, ND Snooping supports not only manual gateway information configuration but also automatic gateway information acquisition.

  A gateway is one of key nodes in a network. ND Snooping supports ND guard against gateway address spoofing attacks. That is, ND packets received on untrusted interfaces are checked only to determine whether they are forged ND packets of key nodes, so as to discard forged packets. This significantly reduces the CPU load of network devices, resource consumption, and dependency on other security features, such as the features mentioned in the description about ND guard. Gateway information can be obtained automatically or manually. Key node information is automatically generated from the obtained gateway information to ensure ND guard against gateway address spoofing attacks.

  During automatic gateway information acquisition, ND Snooping allows automatic learning of gateway information by snooping RA packets in the network. If the gateway is changed, ND Snooping supports

automatic update of the gateway information. The whole process is transparent to the network administrator and does not require special configuration. During manual IPv6 network configuration, you can manually add gateway information and information about servers (key nodes) to guard against server address spoofing attacks.

- RA guard

  RA guard is used to guard against RA packet attacks on L2 access devices. On the basis of ND guard against gateway address spoofing attacks, RA guard is used to check RA packets from ND Snooping trusted interfaces based on more detailed rules, for example, check the source MAC address and source IPv6 address in the RA packets. Only RA packets that meet the rules are forwarded.

- SLACC user monitoring

  Users who use SLACC are called SLACC users. During SLACC, the network administrator does not know how many IPv6 users exist in the network and therefore cannot deploy related management policies.

  When a network attack occurs, the network administrator can obtain the attacker's IP address. However, the network administrator can only locate the specific network segment based on the IP address but not locate the specific network device port or physical client. To resolve the preceding problem, you can monitor SLACC users in the network to obtain related user information. SLACC user monitoring can be configured only on untrusted interfaces.

- ND Snooping and CPP

  Network devices consume certain CPU resources to check ND packet security. To prevent attackers from initiating DoS attacks by sending a large number of ND packets, network devices can use the CPU Protect Policy (CPP) function to control the rate and priority of ND packets. After the ND Snooping function is enabled, the CPP function is enabled automatically for ND packets.

- ND Snooping and NFPP

  The CPP function is used for overall control on ND packets. Moreover, the Network Foundation Protection Policy (NFPP) function can be used to limit the rate of ND packets on interfaces more accurately. The NFPP function takes effect only to ND packets destined for the CPU.

1.1.3 Protocols and Standards

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 4861 Neighbor Discovery for IP version 6 (IPv6)
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 6620 FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses

1.2 Configuration Task Summary

ND Snooping configuration includes the following tasks:

(1) Configuring Basic ND Snooping Functions

(2) (Optional) Configuring ND Guard

(3) (Optional) Configuring ND Logging

1.3 Configuring Basic ND Snooping Functions

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the ND Snooping function to monitor the SLACC process.

ipv6 nd snooping enable

ND Snooping is disabled by default.

(4) (Optional) Disable ND Snooping on a VLAN.

no ipv6 nd snooping enable vlan { *vlan-rng* | *vid* }

After ND Snooping is enabled on a device, it takes effect to all VLANs of the device by default.

(5) (Optional) Configure the lease for an ND Snooping binding entry.

ipv6 nd snooping bind lifetime *time*

The lease time of an ND Snooping binding entry is 300s by default.

(6) (Optional) Configure the capacity for ND Snooping binding entries.

ipv6 nd snooping bind limit *limit*

The capacity configured before delivery is used by default. On interfaces, the capacity for ND snooping binding entries is not limited.

(7) (Optional) Configure the capacity alarm threshold for ND snooping binding entries.

ipv6 nd snooping bind warning-threshold *number*

No capacity alarm threshold is configured for the ND snooping binding entries by default.

(8) (Optional) Configure the waiting time for an address conflict response.

ipv6 nd snooping tentative wait *time*

The default waiting time for an address conflict response is 500 ms.

(9) Enter the interface configuration mode.

interface *interface-type interface-number*

(10) Configure an interface as a ND Snooping trusted interface.

ipv6 nd snooping trust

All interfaces are ND Snooping untrusted interfaces by default.

1.4 Configuring ND Guard

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the number of detection packets to be sent and the interval for sending detection packets when conflicted packets are received.

ipv6 nd snooping detect packet *number* **interval** *time*

Two detection packets are sent at an interval of 250 ms by default.

(4) (Optional) Configure the waiting time for a detection packet response.

ipv6 nd snooping detect wait *time*

The default waiting time for a detection packet response is 500 ms.

(5) (Optional) Configure ND Snooping to work only in ND packet validity check mode.

ipv6 nd snooping nd-check only

ND Snooping is not configured to work only in ND packet validity check mode by default.

After this function is enabled, no ND Snooping entry is generated.

(6) (Optional) Configure the prefix for static IPv6 addresses.

ipv6 nd snooping prefix vlan *vlan-id ipv6-address/prefix-length*

No prefix is configured for static IPv6 addresses by default.

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Enable ND guard against address spoofing attacks.

ipv6 nd snooping check address-resolution

ND guard against address spoofing attacks is disabled by default.

1.5 Configuring ND Logging

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of logging ND Snooping key information.

ipv6 nd snooping log enable

The function of logging ND Snooping key information is disabled by default.

(4) (Optional) Configure the capacity of ND Snooping key information logs.

ipv6 nd snooping log limit *number*

A maximum of 1000 ND Snooping key information logs can be recorded by default.

(5) Enable the function of prompting ND Snooping key information.

ipv6 nd snooping syslog enable

The function of prompting ND snooping key information is disabled by default.

(6) (Optional) Configure the frequency of ND Snooping key information prompts.

ipv6 nd snooping syslog frequency *number*

A maximum of 5 prompts for ND snooping key information are provided every second by default.

1.6 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** command to clear information.

Run the **debug** command to output debugging information.

Caution

- Running the **clear** command may lose vital information and thus interrupt services.
- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
show ipv6 nd snooping prefix	Displays snooped prefix information.
show ipv6 nd snooping binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Displays snooped users with IPv6 stateless addresses.
show ipv6 nd snooping log	Displays ND Snooping key information logs recorded in the memory.
show ipv6 nd snooping packet	Displays ND Snooping packet statistics on an interface.
clear ipv6 nd snooping prefix [**vlan** *vid*]	Clears all prefixes or prefixes snooped in a VLAN.
clear ipv6 nd snooping binding [**vlan** *vid*]	Clears SLACC users.
clear ipv6 nd snooping packet [**interface** *interface-id*]	Clears all packet statistics or packet statistics on an interface.
debug ipv6 nd snooping	Debugs ND Snooping events.

1.7 Configuration Examples

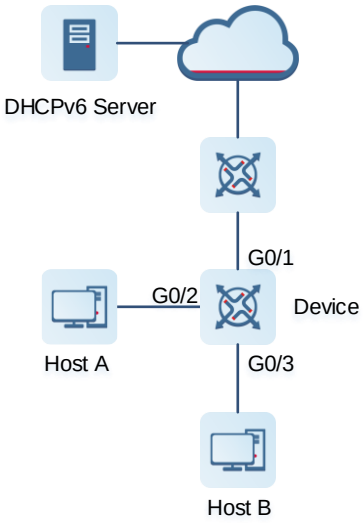
1.7.1 Configuring ND Guard

1. Requirements

Hosts use DHCPv6 to assign IPv6 addresses and enable DHCPv6 Snooping. They also need ND guard against RA attacks and address spoofing attacks.

2. Topology

Figure 1-1 Configuring ND Guard



3. Notes

- Enable ND Snooping.
- Configure trusted interfaces.
- Enable only ND guard against address spoofing attacks.

4. Procedure

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd snooping enable
Device(config)# interface gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ipv6 nd snooping trust
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# interface gigabitethernet 0/2
Device(config-if-GigabitEthernet 0/2)# ipv6 nd snooping check address-resolution
Device(config-if-GigabitEthernet 0/2)# exit
Device(config)# interface gigabitethernet 0/3
Device(config-if-GigabitEthernet 0/3)# ipv6 nd snooping check address-resolution
```

5. Configuration Files

Device configuration file

```
hostname Device
!
ipv6 nd snooping enable
!
interface GigabitEthernet 0/1
 ipv6 nd snooping trust
```

```
!
interface GigabitEthernet 0/2
 ipv6 nd snooping check address-resolution
!
interface GigabitEthernet 0/3
 ipv6 nd snooping check address-resolution
!
end
```

Contents

1 Configuring TCP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 6
1.2 Configuration Task Summary 6
1.3 Configuring TCP SYN Packet Timeout Period 6
1.3.1 Overview 6
1.3.2 Restrictions and Guidelines 6
1.3.3 Procedure 7
1.4 Configuring a TCP Window Size 7
1.4.1 Overview 7
1.4.2 Restrictions and Guidelines 7
1.4.3 Procedure 7
1.5 Configuring the Sending of TCP Reset Packets Upon the Receiving of Port Unreachable Messages 8
1.5.1 Overview 8
1.5.2 Restrictions and Guidelines 8
1.5.3 Procedure 8
1.6 Configuring MSS for a TCP Connection 8
1.6.1 Overview 8
1.6.2 Restrictions and Guidelines 8

1.6.3 Procedure....9

1.7 Configuring the TCP Path MTU Discovery Function....9

1.7.1 Overview....9

1.7.2 Restrictions and Guidelines....9

1.7.3 Procedure....9

1.8 Configuring the MSS Option for TCP SYN Packets....10

1.8.1 Overview....10

1.8.2 Restrictions and Guidelines....10

1.8.3 Procedure....10

1.9 Configuring TCP Connection Exception Detection....10

1.9.1 Overview....10

1.9.2 Procedure....11

1.10 Monitoring....11

1 Configuring TCP

1.1 Introduction

1.1.1 Overview

Transmission Control Protocol (TCP) is a connection-oriented, reliable, and byte stream-based transport layer communication protocol. It is defined in RFC793 of the Internet Engineering Task Force (IETF).

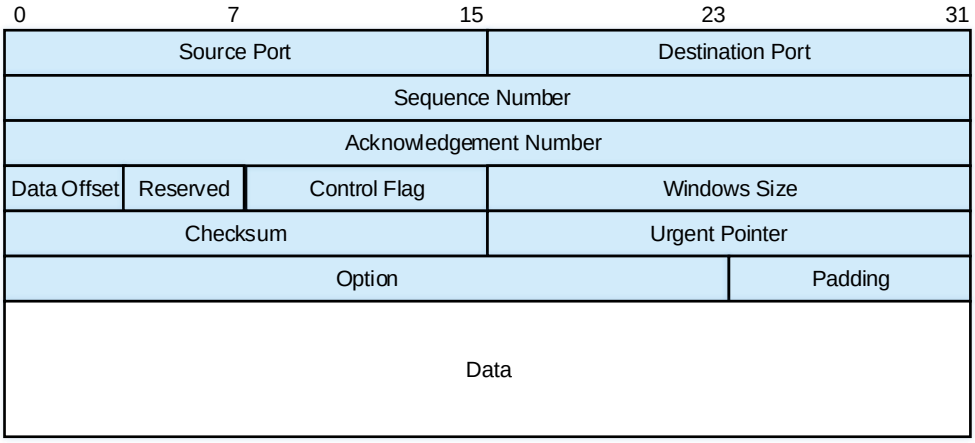
An interconnected network is very different from a single network in that topologies, bandwidth, latency, packet sizes, and other parameters may be entirely different in different parts of the interconnected network. TCP is designed to adapt dynamically to these features of interconnected networks and show robustness in the case of various failures.

- TCP uses a checksum function to check data correctness and validity. The checksum needs to be calculated before transmission and after receiving. Besides, TCP uses the message digest 5 (MD5) authentication to verify data.
- TCP uses sequential transmission, timeout retransmission, and piggyback mechanism to ensure reliability.
- TCP uses the sliding window protocol to control flows. As documented in the protocol, unacknowledged packets in a window need to be retransmitted.
- TCP uses the widely praised TCP congestion control algorithm (also known as the additive increase and multiplicative decrease (AIMD) algorithm) to control congestion.

1.1.2 Principles

1. TCP Header Format

Figure 1-1 TCP Header Format



Field descriptions are as follows:

- **Source Port**: Indicates a 16-bit source port number.
- **Destination Port**: Indicates a 16-bit destination port number.

- **Sequence Number**: Indicates a 32-bit sequence number.
- **Acknowledgment Number**: Indicates a 32-bit acknowledgment sequence number.
- **Data Offset**: Indicates a 4-bit data offset. The value is the length of the TCP header (including the option) divided by 4.
- **Control Flag**: Indicates an 8-bit control flag.

Figure 1-2 Control Flag

0	1	2	3	4	5	6	7
CWR	ECE	URG	ACK	PSH	RST	SYN	FIN

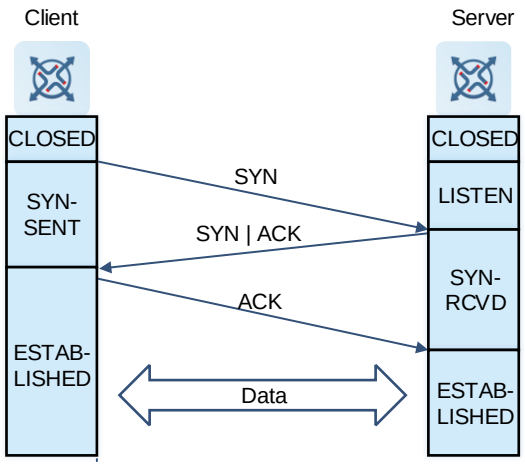
  - Congestion window reduced (**CWR**): The **CWR** flag and the **ECE** flag behind are used for the Explicit Congestion Notification (**ECN**) field in the IP header. When the **ECE** flag is **1**, the peer is notified to make the congestion window smaller.
  - ECN-Echo (**ECE**): The **ECE** flag indicates ECN-Echo. When it is set to **1**, the peer is notified of the congestion from the peer to the local network. When the **ECN** field in the IP header of a received packet is set to **1**, the **ECE** flag in the TCP header is set to **1**.
  - Urgent flag (**URG**): When this bit is set to **1**, the packet contains data that needs urgent processing. Data that needs urgent processing will be further explained in the description of the **Urgent Pointer** field.
  - Acknowledge flag (**ACK**): When this bit is set to **1**, the acknowledgment number is valid. According to the TCP protocol, this bit must be set to **1** except for the SYN packet in the initial establishment of a TCP connection.
  - Push Flag (**PSH**): When this bit is set to **1**, the received data must be immediately transferred to the upper-layer application. When **PSH** is set to **0**, data is buffered instead of being transferred to the upper-layer application immediately.
  - Reset Flag (**RST**): When this bit is set to **1**, the TCP connection must be forcibly closed due to an exception. For example, if a client attempts to establish a TCP connection with a server port that has not provided service externally, the server sends a **RST** packet to the client. In addition, if a device is restarted due to a program crash or power cut, established TCP connections on the device will be closed because all connections will be initialized. In this case, if the peer sends a packet with **RST** set to **1**, the connection is forcibly closed.
  - Synchronize Flag (**SYN**): This bit is used for establishing a connection. If **SYN** is set to **1**, a connection is needed and the initial value of the sequence number is set in the sequence number field.
  - Finish Flag (**FIN**): When this bit is set to **1**, no more data will be sent and disconnection is needed. When the communication ends and disconnection is required, both communication hosts can exchange TCP segments with **FIN** set to **1**. The connection can be closed after each host acknowledges the FIN packet from the peer. However, a host does not have to reply with a FIN packet immediately after receiving a TCP packet with **FIN** set to **1**. Instead, it can wait until all data in the buffer has been successfully sent and is automatically deleted.
- **Window Size**: Indicates 16-bit idle space in the receive buffer. It is used to notify the peer end of a TCP connection of the maximum data length supported by the local end.

- **Checksum**: Indicates a 16-bit TCP checksum.
- **Urgent Pointer**: Indicates a 16-bit field showing the offset of urgent data relative to the value of **Sequence Number**. It is meaningful only when the **URG** flag is set to **1**.
- **Option**: Indicates the option field used to improve the TCP transmission performance. The maximum length is 40 bytes because it is controlled by the data offset (header length). In addition, you are advised to set the **Option** field to an integer multiple of 32 bits.

2. Establishing a TCP Connection

TCP uses the "three-way handshake" mechanism to establish a virtual circuit connection.

Figure 1-3 Establishing a TCP Connection



(1) The client initiates a connection and ends the CLOSED phase. In this case, the server enters the LISTEN phase.

(2) The client sends a TCP SYN packet to the server, and then enters the SYN-SENT phase.

(3) The server receives the SYN packet, ends the LISTEN phase, and responds with an SYN ACK packet. Then, the server enters the SYN-RCVD phase.

(4) The client receives the SYN ACK packet from the server, confirming that the data transmission from the client to the server is normal. The client ends the SYN-SENT phase, and responds with an ACK packet. Then, the client enters the ESTABLISHED phase.

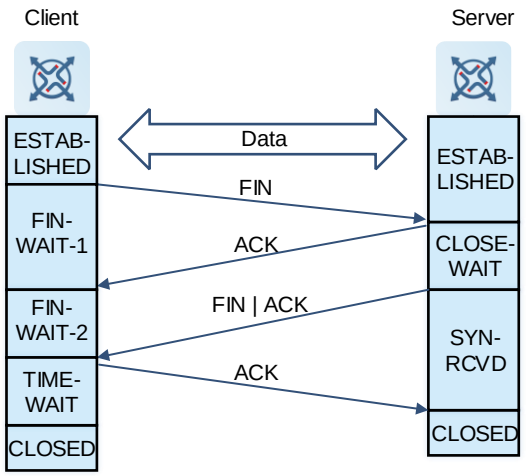
(5) The server receives the ACK packet from the client, confirming that the data transmission from the server to the client is normal. The server ends the SYN-SENT phase, and enters the ESTABLISHED phase.

(6) So far, the three-way handshake is completed, the TCP client and server establish a connection successfully and are ready for data transmission.

3. Releasing a TCP Connection

TCP uses the "four-way wavehand" mechanism to release a virtual circuit connection.

Figure 1-4 Releasing a TCP Connection



(1) To release a connection, the client sends a TCP FIN packet to the server. The client enters the FIN-WAIT-1 phase and stops sending data to the server. At this moment, the client can still receive data from the server.

(2) The server receives the FIN packet, ends the ESTABLISHED phase, enters the CLOSE-WAIT phase, and responds with an ACK packet.

(3) The client receives the ACK packet from the server, confirming that the server has received the connection release request from the client. Then, the client ends the FIN-WAIT-1 phase and enters the FIN-WAIT-2 phase.

(4) After sending the ACK packet, the server goes through the Closed-Wait phase, and sends a FIN ACK packet to the client. At this moment, the server has stopped sending data to the client, but can still receive data from the client.

(5) The client receives the TCP packet from the server, ends the FIN-WAIT-2 phase, enters the TIME-WAIT phase, and sends the ACK packet to the server.

(6) After waiting for a certain period of time, the client ends the TIME-WAIT phase and enters the CLOSED phase. The "four-way wavehand" is completed.

4. SYN Packet Retransmission Upon Timeout

If the server does not reply with an SYN ACK packet after the client sends an SYN packet, the client keeps retransmitting the SYN packet for certain times or until the timeout period expires.

If the server replies with an SYN ACK packet after the client sends an SYN packet but the client does not reply with an ACK packet, the server keeps retransmitting the SYN ACK packet for certain times or until the timeout period expires. This may be SYN flooding.

5. TCP Sliding Window

The TCP sliding window is the receive buffer used to buffer data from the peer. The data will be subsequently read by applications. The TCP window size reflects the size of idle space in the receive buffer. For bulk-data connections, enlarging the window size dramatically promotes TCP transmission performance.

6. MSS

The maximum segment size (MSS) refers to the maximum length of data payload in a TCP segment, excluding the TCP option.

Three-way handshake used for establishing a TCP connection needs MSS negotiation. Both parties of the connection add the MSS option to SYN packets. The option indicates the maximum size of a segment that can be received by the local end, that is, the maximum size of a segment that can be sent by the peer end. Both parties compare the local MSS value with the MSS value received from the peer end and take the smaller MSS value as the MSS of the connection.

The MSS option value in SYN packets to be sent is calculated as follows:

- IPv4 TCP: MSS = IP MTU of the outbound interface corresponding to the peer IP address – IP header size (20 bytes) – TCP header size (20 bytes).
- IPv6 TCP: MSS = Path MTU corresponding to the peer IPv6 address – IPv6 header size (40 bytes) – TCP header size (20 bytes).

Note

The MSS that actually takes effect is the MSS calculated based on the maximum transmission unit (MTU) or the configured MSS, whichever is smaller.

If a connection supports certain options, the option length after 4-byte alignment should be deducted from the MSS value. For example, 20 bytes need to be deducted if the MD5 option is used because the length of the MD5 option is 18 bytes and the length after alignment is 20 bytes.

7. Path MTU Discovery

The TCP path MTU discovery function stipulated in RFC1191 is used to discover the smallest MTU in a TCP path to prevent fragmentation and reassembly and enhance the network bandwidth utilization. The process of IPv4 TCP path MTU discovery is described as follows:

(1) The TCP source sets the Don't Fragment (DF) bit in the outer IP header in a TCP packet to be sent.

(2) If the outbound interface MTU value of a device in the TCP path is smaller than the IP packet length, the packet will be discarded and an ICMP error packet carrying this outbound interface MTU will be sent to the TCP source.

(3) By parsing the ICMP error packet, the TCP source knows the smallest MTU in the TCP path (that is, path MTU).

(4) The size of subsequent data segments sent by the TCP source will not surpass the MSS, which is calculated as follows: TCP MSS = Path MTU – IP header size – TCP header size.

If the MSS has reached the minimum 32 bytes specified by the system and an ICMP error packet asking the system to reduce the MSS is received again, the system will allow the fragmentation of the packets sent from this TCP connection.

The aging mechanism of the path MTU is as follows:

(1) After receiving an ICMP error packet, the TCP source not only reduces the path MTU value, but also starts an aging timer for the path MTU value.

(5) The system gradually increases the MSS value of TCP according to the MTU table specified in RFC 1191 when the timer expires.

(6) If no ICMP error packet is received within 2 minutes after one increment of the MSS, the system continues the increment until the MSS increases to the MSS value advertised by the peer during the three-way handshake.

8. TCP Keepalive Function

You may enable the keepalive function to check whether the peer end of a TCP connection works normally. If the TCP peer end does not send a packet to the local end within a period of time (namely, idle period), the local end starts sending keepalive packets to the peer end for several consecutive times. If no response packet is received, the local end considers the peer end abnormal and closes the TCP connection.

1.1.3 Protocols and Standards

- RFC 793: Transmission Control Protocol
- RFC 1122: Requirements for Internet Hosts -- Communication Layers
- RFC 1191: Path MTU Discovery
- RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II
- RFC 2385: Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 4022: Management Information Base for the Transmission Control Protocol (TCP)

1.2 Configuration Task Summary

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Optimizing TCP performance
  - Configuring TCP SYN Packet Timeout Period
  - Configuring a TCP Window Size
  - Configuring the Sending of TCP Reset Packets Upon the Receiving of Port Unreachable Messages
  - Configuring MSS for a TCP Connection
  - Configuring the TCP Path MTU Discovery Function
  - Configuring the MSS Option for TCP SYN Packets
- Configuring TCP Connection Exception Detection

1.3 Configuring TCP SYN Packet Timeout Period

1.3.1 Overview

In case of SYN flooding, shortening SYN timeout period can reduce resource consumption. However, it does not work on continuous SYN flooding.

When a device actively requests to establish a connection with an external device, shortening SYN timeout period can reduces users' waiting time, for example, waiting time in the telnet connection.

You may prolong SYN timeout period properly on an unstable network.

1.3.2 Restrictions and Guidelines

Perform the configuration on both ends of a TCP connection.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure SYN timeout.

ip tcp synwait-time *time*

The default timeout period of SYN packets used for connection establishment is 20 seconds.

1.4 Configuring a TCP Window Size

1.4.1 Overview

The TCP receive buffer is used to buffer data from the peer. The data will be subsequently read by applications. The TCP window size reflects the size of idle space in the receive buffer. For bulk-data connections, enlarging the window size dramatically promotes TCP transmission performance.

1.4.2 Restrictions and Guidelines

Perform the configuration on both ends of a TCP connection.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configures a TCP window size.

ip tcp window-size *size*

The default TCP window size is 65,535 bytes.

If the window size is greater than 65535 bytes, window enlarging will be enabled automatically. The window size advertised to the peer is the configured window size or the idle space in the receive buffer, whichever is smaller.

Note

This command applies to both IPv4 TCP and IPv6 TCP.

1.5 Configuring the Sending of TCP Reset Packets Upon the Receiving of Port Unreachable Messages

1.5.1 Overview

In general, when the device distributes a TCP packet, if the TCP connection, to which the packet belongs cannot be identified, the device sends a reset packet to the peer to terminate the TCP connection. This, however, can also become a target for attackers. A large number of TCP port unreachable messages can impose attacks on the device. You can use this command to prevent the sending of TCP reset packets upon the receiving of port unreachable messages.

1.5.2 Restrictions and Guidelines

Perform the configuration on both ends of a TCP connection.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the sending of TCP reset packets after port unreachable messages are received.

ip tcp send-reset

TCP reset packets are sent upon the receiving of port unreachable messages by default.

Note

This command applies to both IPv4 TCP and IPv6 TCP.

1.6 Configuring MSS for a TCP Connection

1.6.1 Overview

TCP negotiates about the MSS value when establishing a connection. The MSS refers to the maximum length of data payload in a TCP segment. If the path MTU discovery function at one end of a TCP connection is not available, the device at this end cannot calculate the size of TCP packets based on the MTU value, and the TCP packets may be discarded due to too long size. To prevent this situation, you can manually set the MSS for TCP packets so that the MSS value negotiated by both ends will not exceed this value and the packets can successfully go through the intermediate networks.

1.6.2 Restrictions and Guidelines

- Perform the configuration on both ends of a TCP connection.
- An excessively small MSS reduces transmission performance. You can promote TCP transmission by increasing the MSS. Configure the MSS by referring to the interface MTU. If the former is bigger than the interface MTU, TCP packets need to be fragmented and reassembled, which reduces the transmission performance.

- If an upper MSS limit is configured, the upper MSS limit that actually takes effect is the MSS calculated based on the MTU or configured MSS, whichever is smaller.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an upper MSS limit.

ip tcp mss *max-segment-size*

The calculated value "IPv4/IPv6 MTU – IPv4/IPv6 header length – TCP header length" is used as the upper MSS limit by default.

Note

This command applies to both IPv4 TCP and IPv6 TCP.

1.7 Configuring the TCP Path MTU Discovery Function

1.7.1 Overview

The path MTU discovery function of TCP is implemented according to RFC1191 to improve the network bandwidth utilization. When TCP is applied to bulk transmit chunk data, this function can improve transmission performance greatly.

As described in RFC1191, after discovering the path MTU, TCP can use a larger MSS to probe a new path MTU at intervals. This interval is specified by using the **age-timer** parameter. When the device discovers a path MTU smaller than the MSS negotiated by both ends of a TCP connection, the device tries to probe a larger path MTU at the configured interval described above. The probe process is stopped when the path MTU reaches the MSS or the user turns off the timer. You may use the **age-timer infinite** parameter to turn off this timer.

1.7.2 Restrictions and Guidelines

Perform the configuration on both ends of a TCP connection.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the path MTU discovery function.

ip tcp path-mtu-discovery [**age-timer** *time* | **age-timer infinite**]

The path MTU discovery function of TCP is disabled by default.

Note

This command applies to only IPv4 TCP. The path MTU discovery of IPv6 TCP is enabled permanently and cannot be disabled.

1.8 Configuring the MSS Option for TCP SYN Packets

1.8.1 Overview

Both ends of a TCP connection negotiate about the MSS value for subsequent TCP transmission during the handshake. After the three-way handshake is successful, a TCP connection is established between both ends, and the devices at both ends forward the TCP packets. The tunnel header is encapsulated when a TCP packet is forwarded. Therefore, the length of the TCP packet may exceed the MSS value negotiated during connection establishment, resulting in packet fragmentation and reducing transmission efficiency.

To avoid packet fragmentation, you may configure the MSS option for TCPv4 SYN packets to be forwarded on the device. After receiving a new TCPv4 SYN packet, the device changes the MSS option value in the TCPv4 SYN packet to the configured value.

1.8.2 Restrictions and Guidelines

You may configure an MSS value with a reference to the interface IP MTU.

This configuration applies to new connections but do not take effect on existing TCP connections.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the MSS option for TCP SYN packets to be forwarded.

(IPv4 network)

ip tcp adjust-mss *max-segment-size*

The MSS option is not configured for TCP SYN packets by default.

(IPv6 network)

ipv6 tcp adjust-mss *max-segment-size*

The MSS option is not configured for TCPv6 SYN packets to be forwarded by default.

1.9 Configuring TCP Connection Exception Detection

1.9.1 Overview

You may enable the TCP keepalive function to check whether the peer works normally.

Suppose that the TCP keepalive function is enabled on a device and default interval, transmission count, and idle period settings are used. If no packet is received from the peer within 15 minutes, the device starts sending keepalive packets every 75 seconds for 6 consecutive times. If the device receives no TCP packet from the peer, it considers the TCP connection invalid and automatically releases the TCP connection.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the TCP keepalive function.

ip tcp keepalive [**interval** *interval*] [**times** *times*] [**idle-period** *time*]

The TCP keepalive function is disabled by default.

This command is no different to the server and client and applies to all TCP connections.

Note

This command applies to both IPv4 TCP and IPv6 TCP.

1.10 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 TCP Monitoring

Command	Purpose
show tcp connect [**local-ip** *ip-address*] [**local-port** *port-number*] [**peer-ip** *ip-address*] [**peer-port** *port-number*]	Displays the basic information about an IPv4 TCP connection.
show tcp connect statistics	Displays the statistics on an IPv4 TCP connection.
show tcp pmtu [**local-ip** *ip-address*] [**local-port** *port-number*] [**peer-ip** *ip-address*] [**peer-port** *port-number*]	Displays the path MTU information of IPv4 TCP.
show tcp port [*port-number*]	Displays the usage of IPv4 TCP port.
show tcp parameter	Displays IPv4 TCP parameters.

Command	Purpose
show tcp statistics	Displays IPv4 TCP statistics.
debug ip tcp packet [**in** | **out**] [**local-ip** *ip-address*] [**peer-ip** *ip-address*] [**global** | **vrf** *vrf-name*] [**local-port** *port-number*] [**peer-port** *port-number*] [**deeply**]	Debugs IPv4 TCP packets.
debug ip tcp transactions [**local-ip** *ip-address*] [**peer-ip** *ip-address*] [**local-port** *port-number*] [**peer-port** *port-number*]	Debugs IPv4 TCP connections.
show ipv6 tcp connect [**local-ipv6** *ipv6-address*] [**local-port** *port-number*] [**peer-ipv6** *ipv6-address*] [**peer-port** *port-number*]	Displays the basic information about an IPv6 TCP connection.
show ipv6 tcp connect statistics	Displays the statistics on an IPv6 TCP connection.
show ipv6 tcp pmtu [**local-ipv6** *ipv6-address*] [**local-port** *port-number*] [**peer-ipv6** *ipv6-address*] [**peer-port** *port-number*]	Displays the path MTU information of IPv6 TCP.
show ipv6 tcp port [*port-number*]	Displays the usage of IPv6 TCP port.
debug ipv6 tcp packet [**in** | **out**] [**local-ipv6** *ipv6-address*] [**peer-ipv6** *ipv6-address*] [**global** | **vrf** *vrf-name*] [**local-port** *port-number*] [**peer-port** *port-number*] [**deeply**]	Debugs IPv6 TCP packets.
debug ipv6 tcp transactions [**local-ipv6** *ipv6-address*] [**peer-ipv6** *ipv6-address*] [**local-port** *port-number*] [**peer-port** *port-number*]	Debugs IPv6 TCP connections.

Contents

1 Configuring IP REF 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 3
1.2 Configuration Task Summary 3
1.3 Configuring REF Load Balancing 3
1.3.1 Overview 3
1.3.2 Procedure 4
1.4 Configuring ECMP to Conduct Load Balancing According to a Fixed Profile 4
1.4.1 Overview 4
1.4.2 Restrictions and Guidelines 4
1.4.3 Procedure 5
1.5 Configuring ECMP to Conduct Load Balancing According to an Enhanced Profile 5
1.5.1 Overview 5
1.5.2 Restrictions and Guidelines 5
1.5.3 Procedure 5
1.6 Monitoring 6
1.7 Configuration Examples 8
1.7.1 Configuring Load Balancing 8

1 Configuring IP REF

1.1 Introduction

1.1.1 Overview

On products that do not support hardware-based forwarding, IPv4/IPv6 packets are forwarded by software. To optimize the forwarding performance of software, the device introduces the IPv4/IPv6 Ruijie Express Forwarding (REF) technology to the software. REF can actively resolve next hops and implement load balancing.

REF maintains two tables: forwarding table and adjacency table. The forwarding table is used to store routing information. The adjacency table, equivalent to the Address Resolution Protocol (ARP) table and IPv6 neighbor table, is used to store link layer information of next hops.

1.1.2 Principles

1. Basic Concepts

- Forwarding table

  A forwarding table, also known as forwarding information base (FIB), is the lookup table where the device determines target devices for data exchange, and there are one-to-one mappings between entries in the FIB and entries in the IP routing table. Since the FIB contains all the necessary routing information, there is no need to maintain the route cache. When the network topology or route changes, the IP routing table is updated, and entries in the FIB change accordingly. During packet forwarding, IP REF selects packet transmission paths according to the forwarding table.

- Adjacency table

  An adjacency table contains output interface information of routed packets, for example, the next hop list, the next component used for packet processing, or the link layer output encapsulation. When a packet matches a certain adjacent node, the packet is directly encapsulated and then the send function of the node is called to forward the packet. For the sake of search and update, an adjacency table is often organized in the form of a hash table. To support routing load balancing, the next hop list of an adjacent node is organized in the form of a load balancing table. The next hop list of an adjacent node may not contain next hop information but may contain indexes of next components used for packet processing (such as other line cards and multi-service cards).

- Active resolution

  REF supports next hop resolution. If the MAC address of the next hop of an Ethernet interface is unknown, REF will actively resolve the next hop.

  IPv4 REF requests the ARP module to resolve the next hop. IPv6 REF requests the neighbor discovery (ND) module to resolve the next hops.

  .

- Packet forwarding path

Packets are routed and forwarded based on their IPv4/IPv6 addresses. If the source and destination IPv4/IPv6 addresses of a packet are specified, the forwarding path of this packet is definite.

2. REF Load Balancing

REF Load balancing is used to distribute traffic load among channels of multiple network devices. In the REF model, a route is a multi-path route when the route prefix is associated with multiple next hops. In this case, the route will be associated with a load balancing table and load balancing will be implemented based on the route weights. When an IP packet matches the load balancing table based on the longest prefix match, REF performs hash calculation based on the IP address of the packet and selects a path to forward the packet.

3. ECMP Load Balancing

Equal cost multiple path (ECMP) load balancing works in such a way that the same packet flow is transmitted by one path and different packet flows are transmitted by multiple equal-cost paths according to the load balancing algorithms, to achieve load balancing.

ECMP differentiates packet flows by using one or several load balancing algorithms based on packet characteristics, such as the source IP address, destination IP address, L4 source port number, and L4 destination port number. It also distributes the same packet flow to the same path for transmission, and different packet flows to equal-cost paths evenly.

For example, in source IP address-based load balancing mode, packets are distributed to different paths based on the source IP addresses of the packets. Packets with different source IP addresses are evenly distributed to equal-cost paths, and packets with the same source IP address are forwarded by the same path.

4. Hash Load Balancing Control

Hash load balancing allows users to control load balancing flexibly in different scenarios. Hash load balancing functions are described as below:

- Elastic hash

  In normal cases, a load balancing cluster interworks with multiple top of rack (ToR) devices via the ECMP, and the ToR devices are required to distribute all packets of a session to the same scheduling server. However, when a server is faulty, all session streams will be reorganized and balanced according to the traditional load balancing mechanism of ToR devices. In this case, packets of the same session may be distributed to two servers. The elastic hash function ensures that, when one link is faulty, traffic on other links is not affected and only the traffic of the faulty link is distributed to other active links, without affecting the traffic of other links. In this way, traffic of a session will only be distributed to the same server.

- Hash algorithm mode setting

  When traffic models are different, an appropriate hash algorithm mode can be set to adapt to different traffic to achieve the optimal load balancing effect.

- Hash disturbance

  Device traffic is balanced using the hash algorithm. For the same stream from two devices of the same type, the same path will be calculated by the load balancing algorithm. When the ECMP is deployed, the same stream from the two devices may be distributed to the same destination device. This is called hash polarization. The hash disturbance factor is used to affect the load balancing algorithm of the device. Different disturbance factors can be configured on different devices so that different paths are calculated for the same stream.

- Hash synchronization

  To ensure network security, a firewall cluster is deployed between the internal and external networks for traffic cleaning. This requires that both the uplink and downlink traffic of a session be transmitted to the same device in the firewall cluster for processing. The source and destination IP addresses contained in the uplink and downlink streams of a session are reversed. If a traditional hash algorithm is used, the uplink and downlink streams will be directed to different firewalls, while hash synchronization can ensure that the same path is calculated for the uplink and downlink streams.

- Hash factor acquisition

  For packets of the Generic Routing Encapsulation (GRE) tunnels, there are inner and outer headers. The hash factor can be obtained from the inner or outer header to achieve better load balancing. For example, when tunnel packets have the same IP address in the outer header but different IP addresses in the inner header, the IP address in the inner header can be specified as a hash factor in order to achieve better load balancing.

1.1.3 Protocols and Standards

RFC 1812: Requirements for IP Version 4 Routers

1.2 Configuration Task Summary

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring REF Load Balancing
- Configuring ECMP to Conduct Load Balancing According to a Fixed Profile
- Configuring ECMP to Conduct Load Balancing According to an Enhanced Profile

1.3 Configuring REF Load Balancing

1.3.1 Overview

REF Load balancing is used to distribute traffic load among channels of multiple network devices. REF supports load balancing of packets. In the REF model, a route is a multi-path route when the route prefix is associated with multiple next hops. In this case, the route will be associated with a load balancing table and load balancing will be implemented based on the route weights. When an IP packet matches the load balancing table based on the longest prefix match, REF performs hash calculation based on the IP address of the packet and selects a path to forward the packet.

IP REF supports three load balancing modes, that is, three routing policies:

- The load is balanced based on the destination IP addresses of IP packets and hash calculation is performed on the destination IP addresses of the packets. A path with a greater weight is more likely to be selected. This policy is used by default.
- The load is balanced based on the source and destination IP addresses of IP packets and hash calculation is performed on the source and destination IP addresses of the packets. A path with a greater weight is more likely to be selected.
- The load is balanced based on the source IP addresses of IP packets and hash calculation is performed on the source IP addresses of the packets. A path with a greater weight is more likely to be selected.

1.3.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an IP REF load balancing algorithm.

(IPv4 network)

ip ref load-sharing { **original | original-only** }

The default load balancing algorithm of IPv4 REF is load balancing based on the destination IP addresses.

(IPv6 network)

ipv6 ref load-sharing { **original | original-only** }

The default load balancing algorithm of IPv6 REF is load balancing based on the destination IPv6 addresses.

1.4 Configuring ECMP to Conduct Load Balancing According to a Fixed Profile

1.4.1 Overview

ECMP differentiates packet flows by using one or several load balancing algorithms based on packet characteristics, such as the source IP address, destination IP address, L4 source port number, and L4 destination port number. It also distributes the same packet flow to the same path for transmission, and different packet flows to equal-cost paths evenly.

1.4.2 Restrictions and Guidelines

- The command for configuring a load balancing policy in basic load balancing mode is not different to IPv4 and IPv6.
- When the **enhanced profile** *profile-name* parameter is configured in the **ip ref load-balance** command, load balancing can be performed according to the enhanced profile indicated by *profile-name*. For the enhanced profile configurations, see Configuring ECMP to Conduct Load Balancing According to an Enhanced Profile.
- When running the **ip ref load-balance** command, you can configure the following parameters to select the ECMP load balancing mode using a fixed profile.
  - **enhanced profile** *profile-name*: Performs load balancing based on the field configured in the enhanced profile.
  -
  - **src-dst-ip**: Performs load balancing based on the source and destination IP addresses of packets.
  - **src-dst-ip-src-dst-l4port**: Performs load balancing based on the source IP addresses, destination IP addresses, L4 source port numbers, and L4 destination port numbers of packets.
  - **src-ip**: Performs load balancing based on the source IP addresses of packets.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ECMP load balancing policy.

ip ref load-balance { **enhanced profile** *profile-name* | **src-dst-ip** | **src-dst-ip-src-dst-l4port** | **src-ip** }The load is balanced according to an enhanced profile by default.

(4) (Optional) Enable the elastic hash of ECMP load balancing.

ip ref hash-elasticity enable

Elastic hash of ECMP load balancing is disabled by default.

1.5 Configuring ECMP to Conduct Load Balancing According to an Enhanced Profile

1.5.1 Overview

The enhanced load balancing mode allows users to define load balancing profiles and combine multiple fields of different types of packets for load balancing.

In enhanced load balancing mode, a device first determines the type of packets to be transmitted and performs load balancing based on the specified packet fields. For example, if IPv4 packets containing changing source IP addresses need to be output through an aggregate port, configure the device to perform load balancing based on the specified source IP address field in IPv4 packets.

Configure this function on aggregation or core switches that support enhanced load balancing, and specify parameters to achieve load balancing.

1.5.2 Restrictions and Guidelines

- **dst-ip**: Performs load balancing based on the destination IP addresses of incoming packets.
- **l4-dst-port**: Performs load balancing based on the L4 destination port numbers of incoming packets.
- **l4-src-port**: Performs load balancing based on the L4 source port numbers of incoming packets.
- **protocol**: Performs load balancing based on the protocol types of incoming packets.
- **src-ip**: Performs load balancing based on the source IP addresses of incoming packets.
- **src-port**: Performs load balancing based on the source port numbers of incoming packets.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Rename the enhanced profile and enter the enhanced profile configuration mode of REF load balancing.

ip-ref-load-balance-profile *profile-name*

The default name of the enhanced profile is **default**.

(4) Configure the enhanced profile for load balancing. Perform at least one of the following configuration steps:

- Configure the load balancing mode for IP packets.

  (IPv4 network)

  ipv4 field [**dst-ip**] [**l4-dst-port**] [**l4-src-port**] [**protocol**] [**src-ip**] [**src-port**]

  The load is balanced based on the source IP addresses, destination IP addresses, L4 source port numbers, and L4 destination port numbers of packets by default.

  (IPv6 network)

  ipv6 field [**dst-ip**] [**l4-dst-port**] [**l4-src-port**] [**protocol**] [**src-ip**] [**src-port**]

  The load is balanced based on the source IP addresses, destination IP addresses, L4 source port numbers, and L4 destination port numbers of packets by default.

- Configure the hash disturbance factor.

  hash-disturb *string*

  The hash disturbance function of load balancing is disabled by default.

- Enable hash synchronization.

  hash-symmetrical { **ipv4 | ipv6** }

  Hash synchronization is disabled by default.

1.6 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** command to clear information.

Caution

Running the **clear** command may lose vital information and thus interrupt services.

Table 1-1 Monitoring

Command	Purpose
show ip ref packet statistics	Displays current packet statistics of IPv4 REF.
clear ip ref packet statistics	Clears current packet statistics of IPv4 REF.
show ip ref adjacency [**glean** | **local** | *ip-address* | **interface** *interface-type interface-number* | **discard** | **statistics**]	Displays information about the specified glean adjacencies, local adjacencies, adjacency of a specified IP address, adjacencies associated with a specified interface, and all adjacent nodes of IPv4 REF.

Command	Purpose
show ip ref resolve-list	Displays the next hop resolved by IPv4 REF.
show ip ref exact-route [**vrf** *vrf-name*] *source-ip-address destination-ip-address*	Displays the actual forwarding path of a specified packet.
show ip ref route [**vrf** *vrf-name*] [**default** | *ipv4-address mask* | **statistics**]	Displays routing information in the IPv4 REF table. The parameter **default** indicates that information about the default route will be displayed.
show ip ref route detail *ipv4-address* [**vrf** *vrf-name*]	Displays details about the current IPv4 route.
show ip ref load-balance	Displays the configuration of the ECMP load balancing using a fixed profile.
show ip ref-load-balance-profile [*profile-name*]	Displays the configuration of the ECMP load balancing using an enhanced profile.
ip ref synchronize all	Synchronizes IPv4 routes between the hardware and software REF.
show ipv6 ref packet statistics	Displays current packet statistics of IPv6 REF.
clear ipv6 ref packet statistics	Clears current packet statistics of IPv6 REF.
show ipv6 ref adjacency [**glean** | **local** | *ipv6-address* | **interface** *interface-type interface-number* | **discard** | **statistics**]	Displays information about the specified glean adjacencies, local adjacencies, adjacency of a specified IPv6 address, adjacencies associated with a specified interface, and all adjacent nodes of IPv6 REF.
show ipv6 ref resolve-list	Displays the next hop resolved by IPv6 REF.
show ipv6 ref exact-route [**vrf** *vrf-name*] *source-ipv6-address destination-ipv6-address*	Displays actual the forwarding path of a specified IPv6 packet.
show ipv6 ref route [**vrf** *vrf-name*] [**default** | **statistics** | *ipv6-address/prefix-length*]	Displays route information in the IPv6 REF table. The parameter **default** indicates that information about the default route will be displayed.
show ipv6 ref route detail *ipv6-address* [**vrf** *vrf-name*]	Displays details about the current IPv6 route.

Command	Purpose
ipv6 ref synchronize all	Synchronizes IPv6 routes between the hardware and software REF.

1.7 Configuration Examples

1.7.1 Configuring Load Balancing

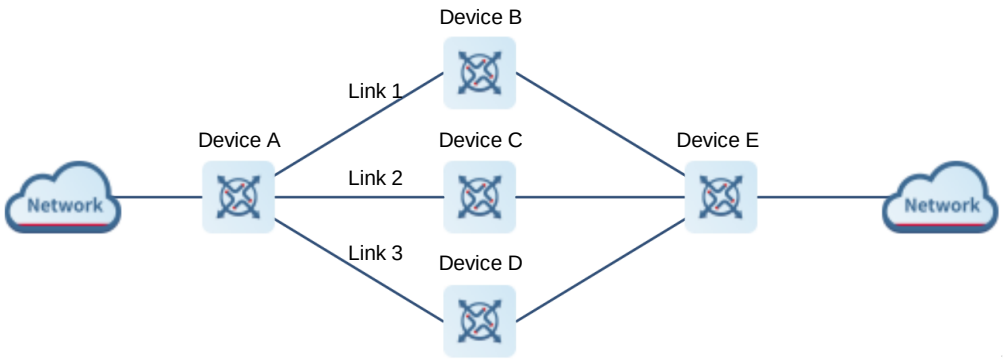
1. Requirements

As shown in Figure 1-1, device A and device E run REF, and device B, device C and device D are forwarding devices.

Device A communicates with device E. Link 1, link 2, and link 3 are three equal-cost links. A specific load balancing algorithm is configured on device A so that traffic is balanced by these three equal-cost links.

2. Topology

Figure 1-1 Topology of Configuring an ECMP Load Balancing Policy



3. Notes

- Configure a policy of load balancing using a fixed profile on device A. Configure the load balancing mode, enable the elastic hash of ECMP load balancing, and configure the ECMP hash algorithm mode.
- Configure a policy of load balancing using an enhanced profile on device A: Rename the ECMP load balancing profile, configure the load balancing mode for IPv4 packets, configure the load balancing mode for IPv6 packets, configure the hash disturbance factor of load balancing, and disable the load balancing hash disturbance function.

4. Procedure

Configure a policy of load balancing using a fixed profile on device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip ref load-balance src-ip
DeviceA(config)# ip ref hash-elasticity enable
```

Configure a policy of load balancing using an enhanced profile on device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip-ref-load-balance-profile rpn
DeviceA(ref-ip-config-load-balance-profile)# ipv4 field src-ip dst-ip
DeviceA(ref-ip-config-load-balance-profile)# ipv6 field src-ip dst-ip protocol
DeviceA(ref-ip-config-load-balance-profile)# hash-disturb A
DeviceA(ref-ip-config-load-balance-profile)# no hash-symmetrical ipv6
```

5. Verification

Run the **show ip ref load-balance** command to display the configuration of load balancing using a fixed profile.

```
DeviceA# show ip ref load-balance
load-balance          : src-ip.
  hash-elasticity       : enable.
```

Run the **show ip ref load-balance-profile** command to display the configuration of load balancing using an enhanced profile.

```
DeviceA# show ip ref load-balance-profile
Load-balance-profile: rpn
Packet   Hash Field:
   IPV4: src-ip dst-ip
   IPV6: protocol src-ip dst-ip
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
ip-ref-load-balance-profile rpn
 ipv4 field src-ip dst-ip
 ipv6 field protocol src-ip dst-ip
 hash-disturb A
!
ip ref load-balance src-ip
ip ref hash-elasticity enable
```

IP Routing Configuration

1. IP Routing Basic Configuration
2. Static Route Configuration
3. RIP Configuration
4. RIPng Configuration
5. OSPFv2 Configuration
6. OSPFv3 Configuration
7. IS-IS Configuration
8. BGP Configuration
9. VRF Configuration
10. Routing Policy Configuration
11. PBR Configuration
12. Key Configuration

Contents

1 Configuring IP Routing Basic 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Configuration Task Summary 3
1.3 Configuring Route Limitations 4
1.3.1 Overview 4
1.3.2 Configuration Tasks 4
1.3.3 Configuring the Maximum Number of Equal-Cost Routes 4
1.3.4 Disabling IPv4 Routing 5
1.3.5 Disabling IPv6 Routing 5
1.4 Configuring Fast Convergence of Recursive Routing 5
1.4.1 Overview 5
1.4.2 Configuration Tasks 6
1.4.3 Enabling IPv4 Recursive Routing Fast Convergence 6
1.4.4 Enabling IPv6 Recursive Routing Fast Convergence 6
1.5 Configuring ARP-to-host Conversion 7
1.5.1 Overview 7
1.5.2 Restrictions and Guidelines 7
1.5.3 Configuration Tasks 7
1.5.4 Configuring the Interface to Enable ARP-to-host Conversion 7
1.5.5 Enabling Proxy ARP 7

1.5.6 Configuring BGP Redistributed ARP-host Route 8

1.6 Configuring ND-to-route Conversion 8

1.6.1 Overview 8

1.6.2 Restrictions and Guidelines 8

1.6.3 Configuration Tasks 8

1.6.4 Configuring the Interface to Enable ND Conversion to Route of Fixed-length Mask 9

1.6.5 Configuring Delayed Redistribution of ND-to-route 10

1.6.6 Configuring Tag Attribute of ND-to-route Conversion 10

1.6.7 Configuring to Ignore Warning Log of ND Conversion to Route of Specified Length 11

1.6.8 Configuring ND Proxy 11

1.6.9 Configuring BGP Redistributed ND-Route Route 12

1.7 Configuring BGP Route Deletion During GR 12

1.7.1 Overview 12

1.7.2 Procedure 12

1.8 Monitoring 13

1 Configuring IP Routing Basic

1.1 Introduction

1.1.1 Overview

A router receives a data packet, checks its destination address, and forwards the packet to the next router according to the routing table. The packet arrives at the destination host after being forwarded multiple times by intermediate routers. The forwarding path of the intermediate routers constitutes the routing path information.

Note

In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be Layer-3 switches, routers, or firewalls.

1.1.2 Principles

1. Composition of Routing Table

A router manages the routing table, consolidates routes sent by various routing protocols, and selects and sends preferred routes to the routing table. Routes discovered by various routing protocols are stored in the routing table. The routing table contains the following key items:

Destination: Destination address, used to identify the destination network or destination address of the IP packet.

Mask: Network mask, which identifies the network segment of the destination address together with the destination address.

Protocol: Routing protocol.

Distance: Management distance, identifying the priority of the route for joining the routing table. For the same destination address, routing management will take the route with the smallest management distance as the optimal route. The table below lists the default management distances of different routing protocols.

Table 1-1 Routing Protocols and Default Management Distances

Routing Protocol	Management Distance
Direct route	0
Static route	1
EBGP	20
OSPF	110
IS-IS	115
RIP	120

Routing Protocol	Management Distance
IBGP	200

Metric: Routing cost. For the same management distance, the route with smallest routing cost will be the optimal route.

NextHop: The next-hop IP address, the interface IP address of the packet in the next forwarding route.

Interface: Forwarding interface, indicating from which interface of the local router the packet is forwarded to the next hop.

2. Route Classification

By the source mode, routes are generally divided into the following three categories:

- Direct route: It is the route discovered by a link-layer protocol and is also called interface route.
- Static route: It is manually configured by the network administrator. A static route is easy to configure and less demanding on the system, and therefore applicable to a small-sized network that is stable and has a simple topology. However, when the network topology changes, the static route must be manually reconfigured and cannot automatically adapt to the topological changes.
- Dynamic route: It is the route discovered by a dynamic routing protocol.

3. Route Computation

- Routing function

  Routing functions are classified into IPv4 and IPv6 routing functions. If the routing functions are disabled, a device is equivalent to a host and cannot forward routes.

- Dynamic Route

  A dynamic routing protocol learns remote routes and dynamically updates routes by exchanging routes with neighbors. If a neighbor is the next hop of a route and this neighbor fails, the route fails as well.

  Classified by the scope of action:

  - Interior Gateway Protocol (IGP): Running in an autonomous system. Protocols are Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Intermediate System to Intermediate System (IS-IS).
  - Exterior Gateway Protocol (EGP): Running between different autonomous systems. Protocol is Border Gateway Protocol (BGP).

  Classified by the route computation algorithm:

  - Distance vector routing protocols: Protocols are BGP and RIP.
  - Link state routing protocols: Protocols are OSPF and IS-IS.

- Static route

  On a network with a simple topology, you can configure only static routes to implement internetworking. Appropriate configuration and use of static routes can improve the network performance and guarantee the bandwidth for important network applications.

Whether a static route is active is computed based on the status of the local interface. When the exit interface of a static route is located at Layer-3 and is in Up status (the link status is Up and the IP address is configured), this route is active and can be used for packet forwarding.

A static route can go across VPN routing & forwarding (VRF) instances. The next hop or exit interface of a static route of VRF 1 can be configured on VRF 2.

- ARP-to-host conversion

  Enable ARP-to-host conversion on a specified interface. If the interface is a Layer-3 interface in Up status, ARP entries will be converted into 32-bit host routes on the interface.

4. Optimal Route Selection

- Management distance

  When multiple routing protocols generate routes to the same destination, the priorities of these routes can be determined based on the management distance. A smaller management distance indicates a higher priority.

- Equal-cost route

  If multiple routes to the same destination have different next hops but the same management distance, these routes are mutually equal-cost routes. Packets are distributed among these routes to implement load balancing based on the balanced forwarding policy.

  On a specific device, the total number of equal-cost routes is limited. Routes beyond the limit do not participate in packet forwarding.

  The routing protocols supporting equal-cost route are the static route, RIP, OSPF, IS-IS, and BGP.

- Floating route

  If multiple routes to the same destination have different next hops and different management distances, these routes are mutually floating routes. The route with the smallest management distance will be first selected for packet forwarding. If this route fails, a route with a larger management distance is further selected for forwarding, thus preventing communication interruption caused by a network line failure.

- Routing recursion

  Only the next hop directly connected can be used as the basis of router forwarding, but the next hop may not be directly connected in BGP and static route. In this case, route iteration is needed to query the routing table according to the next-hop address, find a route with the next hop directly connected or outbound interface, and use the route as the basis for forwarding.

1.2 Configuration Task Summary

The configuration of IP routing basic includes the following tasks:

(1) (Optional) Configuring Route Limitations The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring the Maximum Number of Equal-Cost Routes
- Disabling IPv4 Routing
- Disabling IPv6 Routing

(2) (Optional) Configuring Fast Convergence Fast Convergence The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Enabling IPv4 Recursive Routing Fast Convergence
- Enabling IPv6 Recursive Routing Fast Convergence

(3) (Optional) Configuring ARP-to-host Conversion

a Configuring the Interface to Enable ARP-to-host Conversion

b (Optional) Enabling Proxy ARP

c (Optional) Configuring BGP Redistributed ARP-host Route

(4) (Optional) Configuring ND-to-route Conversion

a Configuring the Interface to Enable ND Conversion to Route of Fixed-length Mask

b (Optional) Configuring Delayed Redistribution of ND-to-route

c (Optional) Configuring Tag Attribute of ND-to-route Conversion

d (Optional) Configuring to Ignore Warning Log of ND Conversion to Route of Specified Length

e (Optional) Configuring ND Proxy

f (Optional) Configuring BGP Redistributed ND-Route Route

(5) (Optional) Configuring BGP Route Deletion During GR

1.3 Configuring Route Limitations

1.3.1 Overview

This function limits the number of equal-cost routes and number of static routes, or disables routing.

1.3.2 Configuration Tasks

The route limitation configuration tasks are as follows and optional. Select tasks for configuration according to actual condition.

- Configuring the Maximum Number of Equal-Cost Routes
- Disabling IPv4 Routing
- Disabling IPv6 Routing

1.3.3 Configuring the Maximum Number of Equal-Cost Routes

1. Overview

Run this command to configure the maximum number of next hops in the equal-cost route.

2. Restrictions and Guidelines

In load balancing mode, the number of routes on which traffic is balanced does not exceed the configured number of equal-cost routes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of equal-cost routes.

maximum-paths *number*

The maximum number of equal-cost routes are 32 by default.

1.3.4 Disabling IPv4 Routing

1. Overview

When a device functions only as a bridge or VoIP gateway, the IPv4 routing and forwarding function is not required. In this case, the IPv4 routing function of the device can be disabled.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable IPv4 routing.

no ip routing

The IPv4 routing function is enabled by default.

1.3.5 Disabling IPv6 Routing

1. Overview

When a device functions only as a bridge or VoIP gateway, the IPv6 routing and forwarding function is not required. In this case, the IPv6 routing function of the device can be disabled.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable IPv6 routing.

no ipv6 unicast-routing

The IPv6 routing function is enabled by default.

1.4 Configuring Fast Convergence of Recursive Routing

1.4.1 Overview

When link discovery changes or is interrupted, the recursive routing query of dynamic route may converge 2 seconds later. The convergence time is unacceptable in some scenarios with high reliability requirements. When the fast convergence function of recursive routing is enabled, the intermediate next hop information will

be added to the route sending information. Even if the intermediate link fails, it can be sensed by routing management to shorten the convergence time.

1.4.2 Configuration Tasks

The recursive routing configuration tasks are as follows and optional. Select tasks for configuration according to actual condition.

- Enabling IPv4 Recursive Routing Fast Convergence
- Enabling IPv6 Recursive Routing Fast Convergence

1.4.3 Enabling IPv4 Recursive Routing Fast Convergence

1. Overview

Enabling IPv4 recursive routing fast convergence can shorten the convergence time of IPv4 network intermediate link failure to a value less than 1 second.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IPv4 recursive routing fast convergence.

ip recur-route fastswitch-nexthop

The fast convergence function of recursive routing is disabled by default.

(4) Forbid recursion to the default route.

ip recur-route over default-route disable

Recursion to the default route is allowed by default.

1.4.4 Enabling IPv6 Recursive Routing Fast Convergence

1. Overview

Enabling IPv6 recursive routing fast convergence can shorten the convergence time of IPv6 network intermediate link failure to a value less than 1 second.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IPv6 recursive routing fast convergence.

ipv6 recur-route fastswitch-nexthop

1.5 Configuring ARP-to-host Conversion

1.5.1 Overview

If other routing protocols are needed to distribute the direct route or instruct forwarding routes, the information in ARP table can be converted into host routes, and then redistributed by other routing protocols.

1.5.2 Restrictions and Guidelines

- The interface must be a Layer-3 interface in Up status.

1.5.3 Configuration Tasks

ARP-to-host conversion configuration includes the following tasks:

(1) Configuring the Interface to Enable ARP-to-host Conversion

(2) (Optional) Enabling Proxy ARP

(3) (Optional) Configuring BGP Redistributed ARP-host Route

1.5.4 Configuring the Interface to Enable ARP-to-host Conversion

1. Overview

This function can be used to convert ARP entries into 32-bit host routes on a specified interface.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable ARP-to-host conversion on a specified interface.

ip route arp-to-host interface *interface-type interface-number*

The ARP-to-host conversion function is disabled on an interface by default.

1.5.5 Enabling Proxy ARP

1. Overview

After receiving an ARP request, the device uses a proxy to send an ARP response with its own Ethernet MAC address. In this case, hosts communicate with each other through Layer-3 routes.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VLAN interface mode.

interface VLAN *vlan-id*

(4) Enable the proxy ARP.

local-proxy-arp

The local proxy ARP function is disabled by default on the SVI interface.

1.5.6 Configuring BGP Redistributed ARP-host Route

1. Overview

BGP redistributes the host routes converted from the ARP table.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the BGP configuration mode.

router bgp *as-number*

(4) Configure BGP redistributed ARP-host route.

redistribute arp-host

ARP-host routes are not redistributed by default.

1.6 Configuring ND-to-route Conversion

1.6.1 Overview

Similar to ARP-to-host conversion, the device can generate direct route information using neighbor discovery (ND) table entries. Other routing protocols can distribute routes according to the generated direct route information, and can specify the mask length of ND-to-route conversion.

1.6.2 Restrictions and Guidelines

- The interface must be a Layer-3 interface in Up status.

1.6.3 Configuration Tasks

ND-to-route conversion configuration includes the following tasks:

(1) Configuring the Interface to Enable ND Conversion to Route of Fixed-length Mask

(2) (Optional) Configuring Delayed Redistribution of ND-to-route

(3) (Optional) Configuring Tag Attribute of ND-to-route Conversion

(4) (Optional) Configuring to Ignore Warning Log of ND Conversion to Route of Specified Length

(5) (Optional) Configuring ND Proxy

(6) (Optional) Configuring BGP Redistributed ND-Route Route

1.6.4 Configuring the Interface to Enable ND Conversion to Route of Fixed-length Mask

1. Overview

After receiving an ARP request, the device uses a proxy to send an ARP response with its own Ethernet MAC address. In this case, hosts communicate with each other through Layer-3 routes.

2. Restrictions and Guidelines

- If neither the IPv6 network segment nor the IPv6 prefix is specified, the ND learned on the interface generates a 128-bit route by default.

  If no IPv6 network segment is specified and only IPv6 prefix is specified, all NDs on the interface generate the specified IPv6 prefix.

  If the IPv6 network segment is specified but no IPv6 prefix is specified, this network segment generates a 128-bit route by default.

  If both the network segment and IPv6 prefix are specified, when ND is learned, the prefix will be checked to find out the network segment it matches, and the configured IPv6 prefix is generated after the specified network segment matched is found.

  If both the network segment and IPv6 prefix are specified and the IPv6 prefix of an unspecified network segment is configured at the same time, a route will be generated according to the IPv6 prefix of the network segment if the network segment is matched, and a route will be generated according to the IPv6 prefix without network segment if the network segment is not matched.
- If you configure the IPv6 address of an interface before configuring the IPv6 prefix for the network segment of this interface address to generate a route with fixed-length mask, a configuration error occurs when the prefix-len is shorter than or equal to the mask of the IPv6 address. In addition, the IPv6 prefix command for the network segment of this interface address fails. For example, if you first configure IPv6 address 10::1/64 on the interface of VLAN 40, and then configure **ipv6 route nd-to-route interface vlan 40 ipv6-prefix 10::1/58 prefix-len 60** in global configuration mode, the configuration fails.
- If you configure the IPv6 address of an interface before configuring the IPv6 prefix of an unspecified network segment, a configuration error occurs when the IPv6 prefix length is shorter than or equal to the mask length of any of the IPv6 addresses on the interface. In addition, the IPv6 prefix configuration command for the unspecified network segment fails. For example, if you first configure IPv6 address 10::1/64 on the interface of VLAN 40, and then configure **ipv6 route nd-to-route interface vlan 40 prefix-len 60** in global configuration mode, the configuration fails.
- If you configure the IPv6 prefix of an unspecified network segment before configuring the IPv6 address of this interface, syslog is displayed and the IPv6 prefix configuration of the unspecified network segment is canceled when the mask length of one of the IPv6 addresses is longer than or equal to the IPv6 prefix of the unspecified network segment. For example, if you first configure **ipv6 route nd-to-route interface vlan 40 prefix-len 60** in global configuration mode, and then configure address 10::1/64 on the interface of VLAN 40, syslog alarm is displayed and the configuration **ipv6 route nd-to-route interface vlan 40 prefix-len 60** is deleted.
- If you configure the IPv6 prefix of the specified network segment and then configure the IPv6 address of the corresponding network segment of the interface, syslog is displayed and the IPv6 prefix configuration of the specified network segment is canceled when the IPv6 address mask of the corresponding network segment is longer than or equal to the IPv6 prefix of the specified network segment. For example, if you first configure

ipv6 route nd-to-route interface vlan 40 ipv6-prefix 10::1/58 prefix-len 60 in global configuration mode, and then configure the address 10::1/64 on the interface of VLAN 40, the syslog alarm is displayed and the configuration **ipv6 route nd-to-route interface vlan 40 ipv6-prefix 10::1/58 prefix-len 60** is deleted.

- If you configure the IPv6 prefix of an unspecified network segment and the IPv6 prefix of the specified network segment, and then configure the IPv6 address of the interface, please check whether the mask of each IPv6 address is longer than or equal to the IPv6 prefix of the specified/unspecified network segment. If so, syslog is displayed and the IPv6 prefix configuration of the corresponding network segment is canceled. For example, if you first configure **ipv6 route nd-to-route interface vlan 40 prefix-len 62** and **ipv6 route nd-to-route interface vlan 40 ipv6-prefix 10::1/58 prefix-len 60** in global configuration mode, and then configure address 10::1/64 on the interface of VLAN 40, the syslog alarm is displayed and the two configuration commands are removed.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable ND conversion to a route with fixed-length mask on the specified interface.

ipv6 route nd-to-route interface *interface-type interface-number* [**ipv6-prefix** *X:X:X:X::X/<0-128>*] [**prefix-len** *masklen*]

The ND-to-route conversion function is disabled on a specified interface by default.

1.6.5 Configuring Delayed Redistribution of ND-to-route

1. Overview

To prevent route jitter caused by change to an ND entry, you can delay conversion of the ND entry into a route.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure delayed redistribution of ND-to-route.

ipv6 route nd-to-route delay-time *delay-time*

The delayed redistribution function of the routes converted by ND is disabled by default. The delayed redistribution time is 0 seconds.

1.6.6 Configuring Tag Attribute of ND-to-route Conversion

1. Overview

This function sets the tag value of ND-to-route conversion to facilitate subsequent route control and management.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the tag attribute of ND-to-route conversion.

ipv6 route nd-to-route tag *tag-number*

The tag attribute function of the ND-converted route is disabled by default.

1.6.7 Configuring to Ignore Warning Log of ND Conversion to Route of Specified Length

1. Overview

After you configure to ignore the warning log of ND conversion to route of specified length, the alarm that the same port ND generates the same network segment route is ignored. If this command is not configured, the warning log that the same port ND generates the same network segment route is printed (only once). The alarm that different ports generate the same network segment route is not controlled by this function.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure to ignore the warning log of ND conversion to a route of specified length.

ipv6 route nd-to-route warning-ignore

The function of ignoring warning log of ND conversion to a route of specified length is disabled by default.

1.6.8 Configuring ND Proxy

1. Overview

When the device receives an ND request, it will send an ND response. The MAC address of the response is the local Ethernet MAC address, so that the interconnection among different hosts is implemented by Layer 3 routing.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the SVI interface mode.

interface vlan *vlan-id*

(4) Configure the IPv6 address of the SVI interface.

ipv6 address *ipv6-address/prefix-length*

(5) Enable the ND proxy.

local-proxy-nd enable

The local ND proxy is disabled by default on the interface.

1.6.9 Configuring BGP Redistributed ND-Route Route

1. Overview

In BGP protocol mode, this command is used to redistribute ND-route to BGP.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter BGP mode.

router bgp *as-number*

(4) Enter BGP IPv6 address family configuration mode.

address-family ipv6

(5) Configure BGP redistributed ND-Route route.

redistribute nd-route [**route-map** *map-tag*] [**metric** *metric-value*]

By default, BGP does not redistribute ND-Route route.

1.7 Configuring BGP Route Deletion During GR

1.7.1 Overview

When a graceful restart (GR)-enabled router is restarted on the control plane, data forwarding can continue on the forwarding plane. In addition, actions (such as neighbor relationship re-forming and route computation) performed on the control plane do not affect functions of the forwarding plane. If the function is enabled, the BGP route deletion configuration takes effect immediately during GR to prevent routing black hole.

1.7.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure direct deletion of the BGP route during GR.

ip route notify delete always

Deletion of the BGP route is disabled by default.

1.8 Monitoring

Run the **show** commands to check the running status of a configured function and verify the configuration effect.

Run the **debug** command to display the output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** command to clear the routing table cache.

Table 1-2 Monitoring

Command	Purpose
clear ip route [**vrf** *vrf-name*] { ***** | *network* [*mask*] }	Clears the routing table cache.
show ip route [[**vrf** vrf-name] [**arphost** | **aggregate** | **count** | [**ecmp** | **fast-reroute** | **normal**] [*network* [*mask*]] | *network* [*mask* [**longer-prefix**]] | *route-protocol* [*process-id*] | **weight** | **tag**]	Displays the IPv4 routing table.
show ipv6 route [[**vrf** *vrf-name*] [[**fast-reroute**] *ipv6-prefix* / *prefix-length* [**longer-prefixes**] | *route-protocol* [*process-id*] | **weight**]]	Displays the IPv6 routing table.
show ip route [**vrf** *vrf-name*] **recursive** *ipv4-network/mask-length*	Displays the recursive information of an IP route.
show ip route [**vrf** *vrf-name*] **static bfd**	Displays the BFD correlation information of an IP route.
show ip route [**vrf** *vrf-name*] **summary**	Displays the statistics of a single routing table.
show ip route [**vrf** *vrf-name*] **track-table**	Displays the track information of IPv4 route correlation.
show ipv6 route [**vrf** *vrf-name*] **static bfd**	Displays the BFD correlation information of an IPv6 route.
show ipv6 route [**vrf** *vrf-name*] **summary**	Displays the statistics of all the IPv6 routing tables.
show route-res usage [**all** | **slot** *slot-id*]	Displays the usage of routing resources.
debug nsm kernel ucast-v4	Debugs IPv4 route management.
debug nsm kernel ucast-v6	Debugs IPv6 route management.
debug nsm kernel frr	Debugs fast reroute management.

Command	Purpose
debug nsm kernel default-network	Debugs default network management.
debug nsm events	Debugs internal events of route management.
debug nsm packet send	Debugs sending of route management and routing protocol messages.
debug nsm packet recv	Debugs receiving of route management and routing protocol messages.

Contents

1 Configuring Static Route 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Configuration Task Summary 2
1.3 Configuring Static Routes 3
1.3.1 Overview 3
1.3.2 Restrictions and Guidelines 3
1.3.3 Configuration Tasks 3
1.3.4 Configuring an IPv4 Static Route 4
1.3.5 Configuring an IPv6 Static Route 4
1.4 Configuring Static Gateway 5
1.4.1 Overview 5
1.4.2 Configuration Tasks 5
1.4.3 Configuring the IPv4 Gateway 5
1.4.4 Configuring the IPv6 Gateway 5
1.4.5 Configuring the IPv4 Default Gateway with Static Route 6
1.4.6 Configuring the IPv6 Default Gateway with Static Route 6
1.4.7 Configuring the IPv4 Default Network with Static Route 7
1.5 Configuring Route Limitations 7
1.5.1 Overview 7
1.5.2 Configuration Tasks 7

1.5.3 Configuring the Maximum Number of IPv4 Static Routes 7

1.5.4 Configuring the Maximum Number of IPv6 Static Routes 8

1.5.5 Prohibiting Static Routing Across VRFs 8

1.5.6 Configuring the Maximum Number of VRF Routes 8

1.6 Correlating a Static Route with BFD 9

1.6.1 Overview 9

1.6.2 Restrictions and Guidelines 9

1.6.3 Configuration Tasks 9

1.6.4 Configuring Correlation of IPv4 Static Routes with BFD 9

1.6.5 Configuring Correlation of IPv6 Static Routes with BFD 10

1.7 Configuring Static Fast Reroute 10

1.7.1 Overview 10

1.7.2 Restrictions and Guidelines 10

1.7.3 Procedure 10

1.8 Configuring Correlation of Static Routes with ARP 11

1.8.1 Overview 11

1.8.2 Procedure 11

1.9 Monitoring 11

1.10 Configuration Examples 12

1.10.1 Configuring an IPv4 Static Route 12

1.10.2 Configuring Correlation of IPv4 Static Routes with Track 16

1.10.3 Configuring Correlation of Static Routes with BFD 18

1.10.4 Configuring Fast Reroute 20

1 Configuring Static Route

1.1 Introduction

1.1.1 Overview

A static route is manually configured by a network administrator. A static route is easy to configure and less demanding on the system, and therefore applicable to a small-sized network that is stable and has a simple topology. Appropriate configuration and use of static routes improves the network performance and guarantees the bandwidth for important network applications. However, when the network topology changes, the static route must be manually reconfigured and cannot automatically adapt to the topological changes.

Note

In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be Layer-3 switches, routers, or firewalls.

1.1.2 Principles

1. Static Route Basic

Whether a static route is active is computed based on the status of the local interface. When the exit interface of a static route is located at Layer-3 and is in Up status (the link status is Up and the IP address is configured), this route is active and can be used for packet forwarding.

A static route can go across VPN routing & forwarding (VRF) instances. The next hop or exit interface of a static route of VRF 1 can be configured on VRF 2.

A static route consists of two parts:

- Destination IP address and mask: The destination IP address of the packet is matched according to the destination address and mask, and the longest matching principle is adopted. The mask can be represented in dotted decimal form or using mask length.
- Outbound interface or next hop address: The next hop of a static route can be the IP address of the outbound interface or next hop router. On a point-to-point network, specifying the outbound interface indirectly determines the next hop router. However, on the Non Broadcast Multiple Access (NBMA) or broadcast network, using an outbound interface as the next hop will lead to multiple next hops. Therefore, you are advised to set the IP address for the next hop router on the NBMA and broadcast networks.

2. Default Route

In a forwarding routing table, the route with the destination network segment 0.0.0.0 and the subnet mask 0.0.0.0 is the default route. Packets that cannot be forwarded by other routes will be forwarded by the default route. The default route can be statically configured or generated by a dynamic routing protocol.

- Default gateway

  After the IP routing function is disabled, run the **ip default gateway** command to generate a default route.
- Static default route

On a device, a static route with the network segment 0.0.0.0 and the subnet mask 0.0.0.0 is configured to generate a default route.

- Default network

  The default network is configured to generate a default route. If the **ip default-network** command is configured to specify a network (a classful network, such as a Class A, B, or C network), and this network exists in the routing table, the router will use this network as the default network and the next hop of this network is the default gateway. As the network specified by the **ip default-network** command is a classful one, if this command is used to identify a subnet in a classful network, the router automatically generates a static route of the classful network instead of any default route.

3. Static route reliability

When a device on a network is faulty, some routes become unreachable, resulting in traffic interruption. If connectivity of the next hop can be detected in real time, the route can be re-computed when a fault occurs, or traffic can be switched over to the standby route.

- Correlation with track

  A track object is an abstract concept. It can be used to trace whether an IP address is reachable or whether an interface is Up. If a dynamic routing protocol or a static route is correlated with the Track function, the dynamic routing protocol or the static route can quickly learn whether the next hop is reachable so as to respond quickly.

- Correlation with BFD

  The bidirectional forwarding detection (BFD) protocol provides a light-load and fast method for detecting the connectivity of the forwarding path between two adjacent routers. If a dynamic routing protocol or a static route is correlated with the BFD function, the dynamic routing protocol or the static route can quickly learn whether the next hop is reachable so as to respond quickly.

  Note

  The detection performance of BFD is better than that of Track.

- Correlation with ARP

  If a static route is correlated with the ARP function, when the ARP does not exist, the static route can quickly learn that the next hop is unreachable so as to respond quickly.

- Fast reroute

  Fast reroute provides a standby route. When a dynamic routing protocol or a static route detects that the next hop is unreachable, it immediately switches traffic over to the standby route to recover communication.

1.2 Configuration Task Summary

The configuration of static route includes the following tasks:

(1) Configuring Static Routes

- Configuring an IPv4 Static Route
- Configuring an IPv6 Static Route

(2) (Optional) Configuring Static Gateway The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring the IPv4 Gateway
- Configuring the IPv6 Gateway
- Configuring the IPv4 Default Gateway with Static Route
- Configuring the IPv6 Default Gateway with Static Route
- Configuring the IPv4 Default Network with Static Route

(3) (Optional) Configuring Route Limitations The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring the Maximum Number of IPv4 Static Routes
- Configuring the Maximum Number of IPv6 Static Routes
- Prohibiting Static Routing Across VRFs
- Configuring the Maximum Number of VRF Routes

(4) (Optional) Correlating a Static Route with BFD The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring Correlation of IPv4 Static Routes with BFD
- Configuring Correlation of IPv6 Static Routes with BFD

(5) (Optional) Configuring Static Fast Reroute

(6) (Optional) Configuring Correlation of Static Routes with ARP

1.3 Configuring Static Routes

1.3.1 Overview

Generate a static route in the routing table. The static route can be used to forward packets to a remote network.

1.3.2 Restrictions and Guidelines

- If the **no ip routing** command is configured, you cannot configure IPv4 static routes on this switch, and existing IPv4 static routes will also be deleted. Before the device is restarted, reconfiguring the **ip routing** command can recover the deleted IPv4 static routes. After the device is restarted, deleted IPv4 static routes cannot be recovered.
- If the **no ipv6 unicast-routing** command is configured, you cannot configure IPv6 static routes on this switch, and existing IPv6 static routes will also be deleted. Before the device is restarted, reconfiguring the **ipv6 unicast-routing** command can recover the deleted IPv6 static routes. After the device is restarted, deleted IPv6 static routes cannot be recovered.
- To correlate a static route with the track function, you must run the **track** command to configure a track object.

1.3.3 Configuration Tasks

The configuration of static route includes the following tasks:

- Configuring an IPv4 Static Route
- Configuring an IPv6 Static Route

1.3.4 Configuring an IPv4 Static Route

1. Overview

In a simple network, you can configure IPv4 static routes to implement internetworking.

2. Restrictions and Guidelines

- If the static route is correlated with track and the Down status of the track object is detected, the static route is not active and does not participate in packet forwarding.
- If the static route is correlated with ARP, but no ARP information of the next hop and egress is detected, the static route is not active and does not participate in packet forwarding.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an IPv4 static route.

ip route [**vrf** *vrf-name*] *network mask* { *ipv4-address* [**global**] | *interface* [*ipv4-address* [**arp** | **global**] *] } [*distance* | **description** *description-text* | [**disabled** | **enabled**] | [**track** *object-number*] [**permanent**] | **tag** *tag* | **weight** *number*] *

No static route is configured by default.

1.3.5 Configuring an IPv6 Static Route

1. Overview

In a simple network, you can configure IPv6 static routes to implement internetworking.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an IPv6 static route.

ipv6 route [**vrf** *vrf-name*] *ipv6-prefix / prefix-length* { *ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }] | *interface* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance*] [**tag** *tag*] [**weight** *number*] [**description** *description-text*]

No IPv6 static route is configured by default.

1.4 Configuring Static Gateway

1.4.1 Overview

The router in an enterprise does not need to obtain all the routing information of the whole Internet. A default route is generated in the routing table and points to the operator gateway, and then the Internet can be accessed. The default route is used to forward packets that cannot be forwarded by other routes.

1.4.2 Configuration Tasks

The default static route configuration tasks are as follows and optional. Select tasks for configuration according to the actual condition.

- Configuring the IPv4 Gateway
- Configuring the IPv6 Gateway
- Configuring the IPv4 Default Gateway with Static Route
- Configuring the IPv6 Default Gateway with Static Route
- Configuring the IPv4 Default Network with Static Route

1.4.3 Configuring the IPv4 Gateway

1. Overview

After running the **no ip routing** command to disable the IPv4 routing function, you can run the **ip default-gateway** command to specify the default IPv4 route. During data interaction, the packet with a destination address not in the local network segment is sent to the default gateway, and the gateway router completes the next-step routing, achieving internetworking between the device and other networks.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the IPv4 gateway.

ip default-gateway *gateway*

No IPv4 default gateway is configured by default.

1.4.4 Configuring the IPv6 Gateway

1. Overview

After running the **no ipv6 unicast-routing** command to disable the IPv6 routing function, you can run the **ipv6 default-gateway** command to specify the default IPv6 route. During data interaction, the packet with a destination address not in the local network segment is sent to the default gateway, and the gateway router completes the next-step routing, achieving internetworking between the device and other networks.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the IPv6 gateway.

ipv6 default-gateway *gateway*

No IPv6 default gateway is configured by default.

1.4.5 Configuring the IPv4 Default Gateway with Static Route

1. Overview

On a device, when the routing for packet sending cannot match an accurate route, the default gateway can be configured so that non-local packets are sent to the default gateway, and then the gateway router completes the next-step routing, achieving internetworking between the local device and other networks.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the IPv4 default gateway with a static route.

ip route [**vrf** *vrf-name*] **0.0.0.0 0.0.0.0** { *ipv4-address* | *interface* [*ipv4-address*] } [*distance*] [**tag** *tag*] [**permanent** | { **track** *object-number* | **arp** }] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**]

By default, no IPv4 default gateway is configured with the static route.

1.4.6 Configuring the IPv6 Default Gateway with Static Route

1. Overview

On a device, when the routing for packet sending cannot match an accurate route, the default gateway can be configured so that non-local packets are sent to the default gateway, and then the gateway router completes the next-step routing, achieving internetworking between the local device and other networks.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the IPv6 default gateway with a static route.

ipv6 route [**vrf** *vrf-name*] **::/0** { *ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }] | *interface* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance*] [**tag** *tag*] [**weight** *number*] [**description** *description-text*]

By default, no IPv6 default gateway is configured with the static route.

1.4.7 Configuring the IPv4 Default Network with Static Route

1. Overview

On a device, when the routing for packet sending cannot match an accurate route, the default gateway can be configured so that non-local packets are sent to the default gateway, and then the gateway router completes the next-step routing, achieving internetworking between the local device and other networks.

2. Restrictions and Guidelines

If the network specified by the **ip default-network** command exists in the routing table, a default route is generated and the next hop to this network is the default gateway. If the network specified by the **ip default-network** command does not exist, the default route is not generated.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the IPv4 default network with a static route.

ip default-network *network*

By default, no IPv4 default network is configured with the static route.

1.5 Configuring Route Limitations

1.5.1 Overview

This function limits the number of equal-cost routes and number of static routes, or disables routing.

1.5.2 Configuration Tasks

The route limitation configuration tasks are as follows and optional. Select tasks for configuration according to the actual condition.

- Configuring the Maximum Number of IPv4 Static Routes
- Configuring the Maximum Number of IPv6 Static Routes
- Prohibiting Static Routing Across VRFs
- Configuring the Maximum Number of VRF Routes

1.5.3 Configuring the Maximum Number of IPv4 Static Routes

1. Overview

This command can be used to configure the maximum number of IPv4 static routes. When the maximum number of IPv4 static routes is reached, no more IPv4 static routes can be configured.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of IPv4 static routes.

ip static route-limit *number*

The configured maximum number of static routes is 1000 by default.

1.5.4 Configuring the Maximum Number of IPv6 Static Routes

1. Overview

This command can be used to configure the maximum number of IPv6 static routes. When the maximum number of IPv6 static routes is reached, no more IPv6 static routes can be configured.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of IPv6 static routes.

ipv6 static route-limit *number*

The configured maximum number of static routes is 1000 by default.

1.5.5 Prohibiting Static Routing Across VRFs

1. Overview

You can use this function to prohibit static IP routing across VRFs. After this command is configured, the static IP routing across VRFs is not active and cannot participate in packet forwarding.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Prohibit static IP routing across VRFs.

no ip route static inter-vrf

Static routing across VRFs is allowed by default.

1.5.6 Configuring the Maximum Number of VRF Routes

1. Overview

This function is used to limit the number of routes running in the default VRF. You can receive warnings only through configuration.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of routes in the default VRF.

maximum routes *limit* { *warn-threshold* | **warning-only** }

The maximum number of routes in the default VRF is not limited by default.

1.6 Correlating a Static Route with BFD

1.6.1 Overview

A static route can quickly detect a route failure with the help of BFD.

1.6.2 Restrictions and Guidelines

- You must configure a static route.
- You must configure BFD session parameters using the **bfd interval min_rx multiplier** command.

1.6.3 Configuration Tasks

The configuration tasks for correlation of static routes with BFD are as follows and optional. Select tasks for configuration according to the actual condition.

- Configuring Correlation of IPv4 Static Routes with BFD
- Configuring Correlation of IPv6 Static Routes with BFD

1.6.4 Configuring Correlation of IPv4 Static Routes with BFD

1. Overview

You can use this function to configure correlation of IPv4 static routes with BFD, quickly sensing change to the destination address link. If the Down status of the BFD session is detected, the IPv4 static route is not active and does not participate in packet forwarding.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure correlation of IPv4 static routes with BFD.

ip route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv4-address*]

Correlation of static routes with BFD is disabled by default.

1.6.5 Configuring Correlation of IPv6 Static Routes with BFD

1. Overview

You can use this function to configure correlation of IPv6 static routes with BFD, quickly sensing change to the destination address link. If the Down status of the BFD session is detected, the IPv6 static route is not active and does not participate in packet forwarding.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure correlation of IPv6 static routes with BFD.

ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv6-address*]

Correlation of static routes with BFD is disabled by default.

1.7 Configuring Static Fast Reroute

1.7.1 Overview

If a routing link fails on the network, the service will be interrupted and cause loss. To avoid the impact of a link failure, the static fast reroute function can be used to switch the link when a link fails.

1.7.2 Restrictions and Guidelines

- You must configure a static route.
- You must configure a route map.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a routing policy.

route-map *route-map-name* [{ **permit** | **deny** } *sequence*]

(4) Create a matching rule.

match interface *interface-type interface-number*

(5) Configure to define a backup route in the route map.

set fast-reroute backup-interface *interface-type interface-number* **backup-nexthop** *ipv4-address*

By default, no backup egress or backup next hop is specified for the matched route.

(6) Return to the global configuration mode.

exit

(7) Configure IPv4 static fast reroute.

ip fast-reroute [**vrf** *vrf-name*] **static route-map** *route-map-name*

The IPv4 static fast reroute function is disabled by default.

(8) Configure IPv6 static fast reroute.

ip fast-reroute [**vrf** *vrf-name*] **static route-map** *route-map-name*

The IPv6 static fast reroute function is disabled by default.

1.8 Configuring Correlation of Static Routes with ARP

1.8.1 Overview

This function is used to configure correlation of static routes with ARP so that ARP requests are actively sent when ARP fails.

1.8.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the interval for actively sending ARP requests.

ip route scan arp interval *request-interval*

The correlation of static routes with ARP is disabled by default, and the ARP request is sent every 5s.

(4) Configure the times of actively sending ARP requests.

ip route scan arp times *request-times*

By default, the correlation of static routes with ARP is disabled, and the ARP request is sent 65,535 times.

1.9 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

Meanwhile, the **debug** command can be used to display the output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

The **clear** command can be used to clear the transmission count of ARP request.

Table 1-1 Monitoring

Command	Purpose
clear ip route arp scan times	Clears the ARP request transmission count and starts counting again.

Command	Purpose
show ip redirects	Displays the default gateway.
show ipv6 redirects	Displays the IPv6 default gateway.

1.10 Configuration Examples

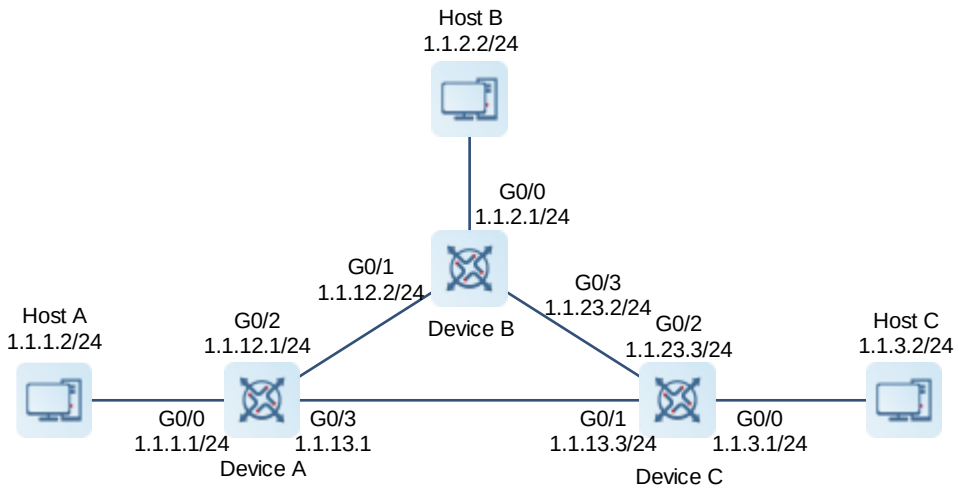
1.10.1 Configuring an IPv4 Static Route

1. Requirements

Configure static routes to make routes on the entire network reachable.

2. Topology

Figure 1-1 Topology for IPv4 Static Routes



3. Notes

- Configure an address on each interface of the device.
- Configure static routes on the device.

4. Procedure

(1) Configure an IP addresses for each interface.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitEthernet 0/0
Device A(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/0)# exit
Device A(config)# interface gigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0
```

```
Device A(config-if-GigabitEthernet 0/2)# exit
Device A(config)# interface gigabitEthernet 0/3
Device A(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/3)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface gigabitEthernet 0/0
Device B(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0
Device B(config-if-GigabitEthernet 0/0)# exit
Device B(config)# interface gigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface gigabitEthernet 0/3
Device B(config-if-GigabitEthernet 0/3)# ip address 1.1.23.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/3)# exit
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface gigabitEthernet 0/0
Device C(config-if-GigabitEthernet 0/0)# ip address 1.1.3.1 255.255.255.0
Device C(config-if-GigabitEthernet 0/0)# exit
Device C(config)# interface gigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip address 1.1.13.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface gigabitEthernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ip address 1.1.23.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/2)# exit
```

(2) Enable the IPv4 static route function.

Configure Device A.

```
Device A(config)# ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.12.2
Device A(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.13.3
```

Configure Device B.

```
Device B(config)# ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.12.1
Device B(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.23.3
```

Configure Device C.

```
Device C(config)# ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.23.2
Device C(config)# ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.13.1
```

5. Verification

Check the routing table of the device and confirm that there are static route entries.

Check the routing table of Device A.

```
Device A# show ip route
```

```
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default

Gateway of last resort is no set
C    1.1.1.0/24 is directly connected, GigabitEthernet 0/0
C    1.1.1.1/32 is local host.
S    1.1.2.0/24 [1/0] via 1.1.12.2, GigabitEthernet 0/2
S    1.1.3.0/24 [1/0] via 1.1.13.3, GigabitEthernet 0/2
C    1.1.12.0/24 is directly connected, GigabitEthernet 0/2
C    1.1.12.1/32 is local host.
C    1.1.13.0/24 is directly connected, GigabitEthernet 0/3
C    1.1.13.1/32 is local host.
```

Check the routing table of Device B.

```
Device B# show ip route
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default

Gateway of last resort is no set
S    1.1.1.0/24 [1/0] via 1.1.12.1, GigabitEthernet 0/0
C    1.1.2.0/24 is directly connected, GigabitEthernet 0/0
C    1.1.2.1/32 is local host.
S    1.1.3.0/24 [1/0] via 1.1.23.3, GigabitEthernet 0/3
C    1.1.12.0/24 is directly connected, GigabitEthernet 0/1
C    1.1.12.2/32 is local host.
C    1.1.23.0/24 is directly connected, GigabitEthernet 0/3
C    1.1.23.2/32 is local host.
```

Check the routing table of Device C.

```
Device C# show ip route
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default

Gateway of last resort is no set
S    1.1.1.0/24 [1/0] via 1.1.13.1, GigabitEthernet 0/2
```

```
S    1.1.2.0/24 [1/0] via 1.1.23.2, GigabitEthernet 0/2
C    1.1.3.0/24 is directly connected, GigabitEthernet 0/0
C    1.1.3.1/32 is local host.
C    1.1.13.0/24 is directly connected, GigabitEthernet 0/1
C    1.1.13.3/32 is local host.
C    1.1.23.0/24 is directly connected, GigabitEthernet 0/2
C    1.1.23.3/32 is local host.
```

6. Configuration Files

- Device A configuration file

```
!
interface gigabitEthernet 0/0
 ip address 1.1.1.1 255.255.255.0
!
interface gigabitEthernet 0/2
 ip address 1.1.12.1 255.255.255.0
!
interface gigabitEthernet 0/3
 ip address 1.1.13.1 255.255.255.0
!
ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.12.2
ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.13.3
!
```

- Device B configuration file

```
!
interface gigabitEthernet 0/0
 ip address 1.1.2.1 255.255.255.0
!
interface gigabitEthernet 0/1
 ip address 1.1.12.2 255.255.255.0
!
interface gigabitEthernet 0/3
 ip address 1.1.23.2 255.255.255.0
!
ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.12.1
ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.23.3
!
```

- Device C configuration file

```
!
interface gigabitEthernet 0/0
 ip address 1.1.3.1 255.255.255.0
!
interface gigabitEthernet 0/1
 ip address 1.1.13.3 255.255.255.0
!
```

```
interface gigabitEthernet 0/2
 ip address 1.1.23.3 255.255.255.0
!
ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.23.2
ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.13.1
!
```

7. Common Errors

- The link on the interface is not Up.
- No IP address is configured for the interface.

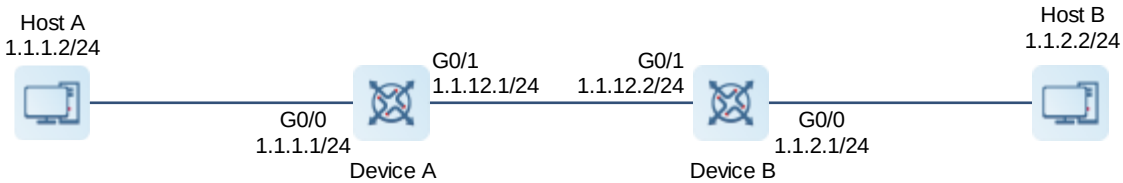
1.10.2 Configuring Correlation of IPv4 Static Routes with Track

1. Requirements

Device A and Device B implement the interworking between Host A 1.1.1.2 and Host B 1.1.2.2 through a static route. To know the link reachability in time, use correlation of IPv4 static routes with track.

2. Topology

Figure 1-2 Topology for Correlating IPv4 Static Routes with Track



3. Notes

- Configure an address on each interface of the device.
- Configure static routes on Device A and Device B, and specify the exit interface or next hop as the interworking interface.
- Correlate static routes with track on Device A and Device B, and check the connectivity of the next hops of static routes.

4. Procedure

(1) Configure an IP address for each interface and start the unicast routing protocol.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/1)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
```

```
Device B(config)# interface gigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
```

(2) Configure the track function.

Configure Device A.

```
Device A(config)# track 2 interface gigabitEthernet 0/1 line-protocol
```

Configure Device B.

```
Device B(config)# track 2 interface gigabitEthernet 0/1 line-protocol
```

(3) Configure correlation of static routes with track.

Configure Device A.

```
Device A(config)# ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.2 track
2
```

Configure Device B.

```
Device B(config)# ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.1 track
2
```

5. Verification

Display the statistics of Track 2.

```
Device A# show track 2
Track 2
Interface gigabitEthernet 0/1
  The state is Up, delayed Down (5 secs remaining)
    1 change, current state last: 300 secs
  Delay up 0 secs, down 0 secs
```

Display the track correlation information and state of an IP route.

```
Device A# show ip route track-table
ip route 1.1.2.0 255.0.0.0 GigabitEthernet 0/1 1.1.12.2 track 2 up
```

6. Configuration Files

- Device A configuration file

```
!
interface gigabitEthernet 0/1
 ip address 1.1.12.1 255.255.255.0
!
track 2 interface gigabitEthernet 0/1 line-protocol
!
ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.2 track 2
!
```

- Device B configuration file

```
!
interface gigabitEthernet 0/1
 ip address 1.1.12.2 255.255.255.0
```

```
!
track 2 interface gigabitEthernet 0/1 line-protocol
!
ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.1 track 2
!
```

7. Common Errors

- The static route is correlated with track, but no track object is configured.

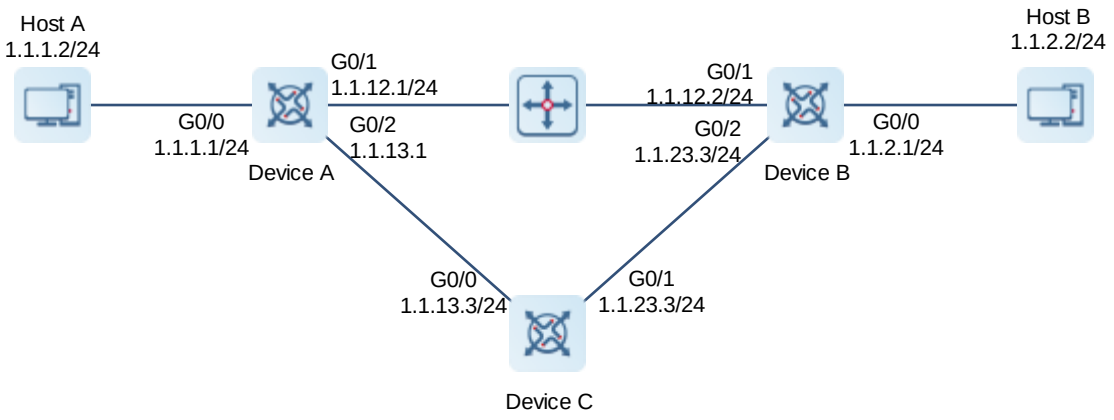
1.10.3 Configuring Correlation of Static Routes with BFD

1. Requirements

Configure static routes for Host A and Host B to realize interworking, where Device A-Device B is the primary link. After BFD is configured, if the primary link fails, packets can switch to Device C quickly to implement communication.

2. Topology

Figure 1-3 Topology for Correlation of Static Routes with BFD



3. Notes

- Configure static routes on Device A, Device B, and Device C, and specify the exit interface or next hop as the interworking interface.
- Configure a BFD session on the interconnect interface between Device A and Device B.
- Correlate static routes with BFD on Device A and Device B, and check the connectivity of the next hops of static routes.

4. Procedure

(1) Configure IP addresses of interfaces (omitted).

(2) Configure static routes to implement internetworking.

Configure Device A.

```
Device A> enable
Device A# configure terminal
```

```
Device A(config)# ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.2
Device A(config)# ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/2 1.1.13.3 40
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.1
Device B(config)# ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/2 1.1.23.3 40
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/0 1.1.13.1
Device C(config)# ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/1 1.1.23.2
```

(3) Configure BFD for an interface.

Configure Device A.

```
Device A(config)# interface gigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# bfd interval 50 min_rx 50 multiplier 3
Device A(config-if-GigabitEthernet 0/1)# exit
```

Configure Device B.

```
Device B(config)# interface gigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# bfd interval 50 min_rx 50 multiplier 3
Device B(config-if-GigabitEthernet 0/1)# exit
```

(4) Configure correlation of static routes with BFD.

Configure Device A.

```
Device A(config)# ip route static bfd gigabitEthernet 0/1 1.1.12.2
```

Configure Device B.

```
Device B(config)# ip route static bfd gigabitEthernet 0/1 1.1.12.1
```

5. Verification

Display the states of BFD neighbors.

```
Device A# show bfd neighbors
OurAddr     NeighAddr    LD/RD   RH/RS   Holdown(mult)  State  Int
1.1.12.1    1.1.12.2     8192/0   Up      0(3   )       Up GigabitEthernet 0/1
```

Display the states of BFD neighbors.

```
Device A# show ip route static bfd
S    1.1.2.0/24 via 1.1.12.2, GigabitEthernet 0/1, BFD state is Up
```

6. Configuration Files

- Device A configuration file

```
!
interface gigabitEthernet 0/1
 bfd interval 50 min_rx 50 multiplier 3
!
```

```
ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.2
ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/2 1.1.13.3 40
!
ip route static bfd gigabitEthernet 0/1 1.1.12.2
!
```

- Device B configuration file

```
!
interface gigabitEthernet 0/1
 bfd interval 50 min_rx 50 multiplier 3
!
ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.1
ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/2 1.1.23.3 40
!
ip route static bfd gigabitEthernet 0/1 1.1.12.1
!
```

- Device C configuration file

```
!
ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/0 1.1.13.1
ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/1 1.1.23.2
!
```

7. Common Errors

- The link on the interface is not Up.
- No IP address is configured for the interface.
- No BFD session parameters are configured.
- No static route is configured.

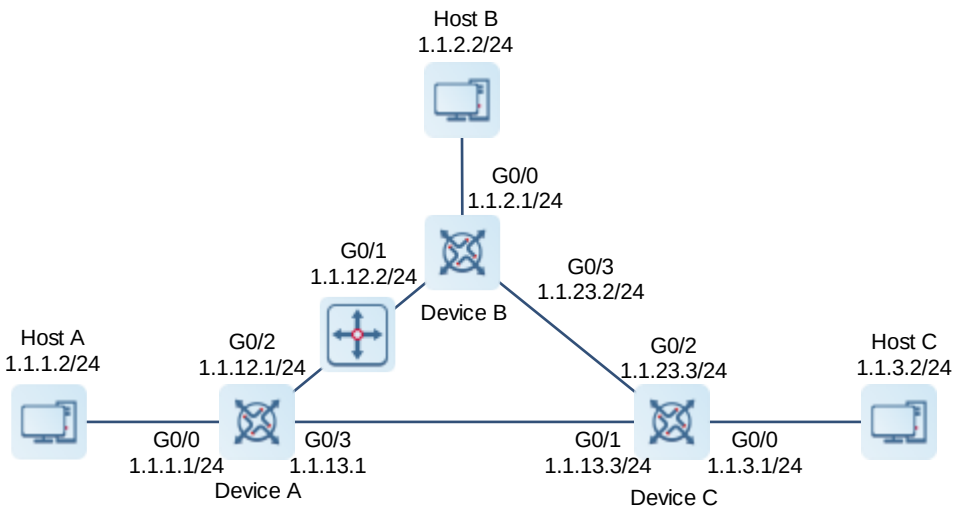
1.10.4 Configuring Fast Reroute

1. Requirements

Device A, Device B, and Device C are interconnected through static routes, and Device A accesses Host C through Device C by default. In consideration of the possible link failure of Device A and Device C, configure fast reroute to quickly switch to the backup link in case of a link failure.

2. Topology

Figure 1-4 Topology for Fast Reroute



3. Notes

- On Device A, configure a static route to the network segment of Host C, and the next hop of the exit interface is Device C.
- On Device A, configure static fast reroute. The next hop of the exit interface of the backup route is Device B.

4. Procedure

(1) Configure an IP address for the router (omitted).

(2) Configure static routes to implement internetworking between all the hosts (omitted).

(3) Configure a route map, and set the next hop of the exit interface of the backup route to Device B.

```
Device A> enable
Device A# configure terminal
Device A(config)# route-map fast-reroute
Device A(config-route-map)# set fast-reroute backup-interface GigabitEthernet 0/2
backup-nexthop 1.1.12.2
```

(4) Configure static fast reroute.

```
Device A(config-route-map)# exit
Device A(config)# ip fast-reroute static route-map fast-reroute
```

5. Verification

Display the primary and backup routes on Device A.

```
Device A# show ip route fast-reroute
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
       Status codes: m - main entry, b - backup entry, a - active entry

Gateway of last resort is no set
S   1.1.3.0 /24 [ma] via 1.1.13.3, GigabitEthernet 0/3
               [b]  via 1.1.12.2, GigabitEthernet 0/2
```

6. Configuration Files

- Device A configuration file

```
!
route-map fast-reroute
set fast-reroute backup-interface GigabitEthernet 0/2 backup-nexthop 1.1.12.2
!
ip fast-reroute static route-map fast-reroute
!
```

7. Common Errors

- The link on the interface is not Up.
- No static route is configured.
- The **match** matching conditions are not configured or are not correctly configured in the road map.

Contents

1 Configuring RIP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 9
1.2 Configuration Task Summary 9
1.3 Configuring Basic Features 10
1.3.1 Overview 10
1.3.2 Restrictions and Guidelines 10
1.3.3 Configuration Tasks 11
1.3.4 Enabling RIP Process 11
1.3.5 Configuring Association with the Local Network 11
1.3.6 Configuring RIP Version 12
1.3.7 Configuring Split Horizon 12
1.3.8 Configuring a Passive Interface 13
1.3.9 Enabling Triggered Updates 13
1.4 Enabling RIP Route Summarization 14
1.4.1 Overview 14
1.4.2 Restrictions and Guidelines 14
1.4.3 Configuration Tasks 14
1.4.4 Configuring to Enable Automatic Route Summarization Function 15

1.4.5 Configuring RIP Route Summarization on an Interface 15

1.5 Configuring RIP Route Filtering Rules..... 16

1.5.1 Overview 16

1.5.2 Restrictions and Guidelines 16

1.5.3 Configuration Tasks 16

1.5.4 Configuring to Filter the Received RIP Routing Information 16

1.5.5 Configuring to Filter the Sent RIP Routing Information 17

1.6 Configuring to Adjust RIP Routing..... 17

1.6.1 Overview 17

1.6.2 Restrictions and Guidelines 18

1.6.3 Configuration Tasks 18

1.6.4 Configuring to Modify the Management Distance of a RIP Route..... 18

1.6.5 Configuring to Increase the Metric of a Received or Sent RIP Route..... 18

1.6.6 Configuring the Default Metric of an External Route Redistributed to RIP 19

1.7 Modifying Timers..... 19

1.7.1 Overview 19

1.7.2 Restrictions and Guidelines 19

1.7.3 Configuration Tasks 20

1.7.4 Configuring to Modify the Update Timer, Invalid Timer, Flush Timer, and Holddown Timer of a RIP Route 20

1.7.5 Configuring the Sending Delay Between RIP Route Update Packets 20

1.8 Configuring RIP Route Distribution..... 21

1.8.1 Overview 21

1.8.2 Restrictions and Guidelines 21

1.8.3 Configuration Tasks 21

1.8.4 Configuring to Advertise a Default Route to Neighbors 21

1.8.5 Configuring to Advertise a Default Route to Neighbors on an Interface 22

1.8.6 Configuring Route Redistribution 23

1.9 Controlling Interaction of RIP Packets 24

1.9.1 Overview 24

1.9.2 Restrictions and Guidelines 24

1.9.3 Configuration Tasks 24

1.9.4 Configuring to Send Unicast RIP Route Update Packets 25

1.9.5 Configuring to Send Broadcast RIPv2 Packets on an Interface 25

1.9.6 Configuring to Allow an Interface to Receive RIP Packets 26

1.9.7 Configuring to Allow an Interface to Send RIP Packets 26

1.9.8 Configuring to Allow an Interface to Send RIP Packets of a Specified Version 27

1.9.9 Configuring to Allow an Interface to Receive RIP Packets of a Specified Version 27

1.10 Configuring to Enable RIPv2 Authentication 28

1.10.1 Overview 28

1.10.2 Restrictions and Guidelines 28

1.10.3 Configuration Tasks 28

1.10.4 Configuring RIP Authentication Mode 28

1.10.5 Configuring a Key Chain for Authentication 29

1.10.6 Configuring a Key Chain for RIP Plain Text Authentication 30

1.11 Configuring BFD Correlation with RIP 30

1.11.1 Overview 30

1.11.2 Restrictions and Guidelines 30

1.11.3 Configuration Tasks 30

1.11.4 Configuring BFD Correlation with RIP Globally 31

1.11.5 Configuring BFD Correlation with RIP on an Interface 31

1.12 Configuring to Enable RIP Fast Reroute 32

1.12.1 Overview 32

1.12.2 Restrictions and Guidelines 32

1.12.3 Procedure 32

1.13 Enabling GR 33

1.13.1 Overview 33

1.13.2 Restrictions and Guidelines 33

1.13.3 Procedure 33

1.14 Configuring to Enable RIP Supernetting Routes 33

1.14.1 Overview 33

1.14.2 Restrictions and Guidelines 33

1.14.3 Procedure 33

1.15 Configuring RIP to Enable Multiple VRF Instances 34

1.15.1 Overview 34

1.15.2 Restrictions and Guidelines 34

1.15.3 Configuration Tasks 34

1.15.4 Configuring a VRF Instance 34

1.15.5 Configuring to Bind a RIP MIB with a VRF Instance 35

1.16 Configuring a Super VLAN to Enable RIP 35

1.16.1 Overview 35

1.16.2 Restrictions and Guidelines 36

1.16.3 Procedure 36

1.17 Enabling Source Address Verification 36

1.17.1 Overview 36

1.17.2 Restrictions and Guidelines 36

1.17.3 Procedure 36

1.18 Monitoring 37

1.19 Configuration Examples 38

1.19.1 Building a RIP Routing Domain 38

1.19.2 Configuring RIP to Prevent Route Loop 43

1.19.3 Configuring External Routes Imported by RIP 45

1.19.4 Configuring Increasing the Metric of a RIP Interface 46

1.19.5 Configuring RIP to Distribute a Summarized Route 48

1 Configuring RIP

1.1 Introduction

1.1.1 Overview

Routing Information Protocol (RIP) is a unicast routing protocol applied to IPv4 networks. RIP-enabled devices exchange routing information to automatically obtain routes to remote networks.

As an Interior Gateway Protocol (IGP), RIP can run only within an autonomous system (AS). RIP is a distance vector routing protocol, which can control packet interaction through UDP (Port 520) and applies to small-scale networks. Due to simplicity, ease of use, and low workload of configuration and maintenance, the RIP routing protocol is widely used for small networks.

1.1.2 Principles

1. Basic Concepts

- IGP and EGP

  IGP runs within an AS. For example, RIP is a type of IGP.

  Exterior Gateway Protocol (EGP) runs between ASs. For example, BGP is a type of EGP.

- Classful routing protocol and classless routing protocol

  Protocols can be classified based on the type of routes supported:

  Classful routing protocol: It supports classful routes. For example, RIPv1 is a classful routing protocol.

  Classless routing protocol: It supports classless routes. For example, RIPv2 is a classless routing protocol.

- RIP timer
  - Update timer: Route update packets are sent regularly, and the update interval is 30s by default.
  - Invalid timer: If an update packet for refreshing the existing route has not been received after 180s (default value), the metric for the route to set to 16, marking the route as invalid.
  - Flush timer: By default, the flush timer is set to 240s, 60s greater than the invalid timer. When the flush timer times out, the route is deleted from the routing table.
  - Hold-down timer: It prevents route loop caused by route flapping. When the device receives a route update with a metric value of 16, the route will be set to hold-down state, and the hold-down timer will be started at the same time. Before the hold-down timer expires, even if an update packet with a metric less than 16 for this route is received, the route will not be updated.

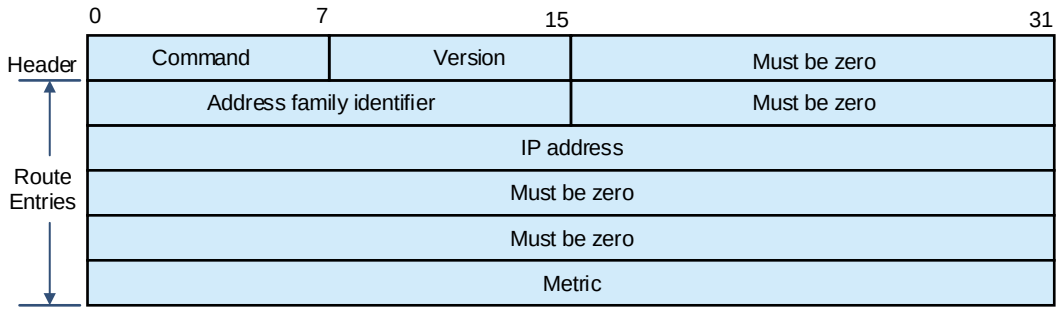
2. RIPv1 and RIPv2

RIP is available in two versions: RIPv1 and RIPv2.

- RIPv1

  RIPv1 packets are broadcast. The broadcast address is 255.255.255.255, and the UDP port ID is 520. No subnet mask is carried in RIPv1 packet, so RIPv1 cannot identify the subnet mask, and supports only classful routes. Meanwhile, RIPv1 does not support routing aggregation and discontinuous subnet.

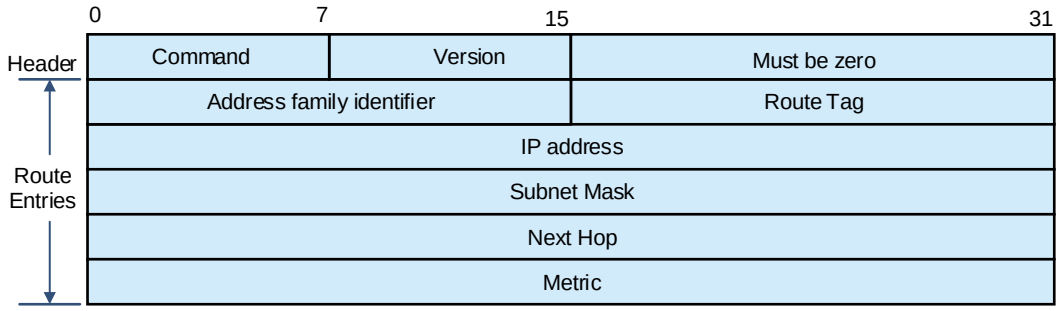
Figure 1-1 RIPv1 Packet Format



- RIPv2

  RIPv2 packets are multicast. The multicast address is 224.0.0.9, and the UDP port ID is 520. RIPv2 can identify the subnet mask, and supports classless routes, summarized route, and supernetting routes. RIPv2 supports plain text authentication and message digest 5 (MD5) authentication. During route redistribution, tags can be added to external routes, and the policy route can control RIP routes according to tags.

Figure 1-2 RIPv2 Packet Format



3. Route Control

Compared with static routing, the dynamic routing protocol shows an advantage, that is, by exchanging routing information, devices can automatically obtain routes to a remote network and update the routes in real time.

- Initialization

  After RIP is enabled on a device, the device sends a request packet to its neighbor device, asking for all routing information, that is, the routing table. After receiving the request packet, the neighbor device returns a response packet containing the local routing table. After receiving the response packet, the device updates the local routing table, and sends an update packet to the neighbor device, informing the neighbor device of the route

update information. After receiving the update packet, the neighbor device updates the local routing table, and sends the update packet to other adjacent devices. After receiving the update advertisement, all devices can obtain and retain the latest routing information.

- Periodical update

  By default, periodical update is enabled for RIP. Adjacent devices exchange complete routing information with each other every 30s, that is, the entire routing table is sent to neighbor devices. One update packet contains at most 25 routes. Therefore, a lot of update packets may be required to send the entire routing table. You can set the sending delay between update packets to avoid loss of routing information.

Note

For every non-local route, if the route is not updated within 180s (Invalid timer), the metric of the route is changed to 16 (unreachable). If the route is still not updated in the next 120s (Flush timer), the route is deleted from the routing table.

- Triggered update

  After the triggered update function is enabled, periodical update is automatically disabled. When routing information changes on a device, the device immediately sends routes related to the change (instead of the complete routing table) to the neighbor device, and use the acknowledgment and retransmission mechanisms to ensure that the neighbor device receives the routes successfully. Compared with periodical update, triggered update helps reduce flooding and accelerates route convergence.

  Events that can trigger update include router startup, interface status change, changes in routing information (such as the metric), and reception of a request packet.

- Route summarization

  When sending routing information to a neighbor device, the RIP-enabled device summarizes subnet routes that belong to the same classful network into a route, and sends the route to the neighbor device. For example, summarize 80.1.1.0/24 (metric = 2) and 80.1.2.0/24 (metric = 3) into 80.0.0.0/8 (metric = 2).

  You can manually specify the aggregation address to summarize routes into a classless route. For example, summarize 80.1.1.0/24 (metric = 2) and 80.1.2.0/24 (metric = 3) into 80.1.0.0/16 (metric = 2).

Note

Only RIPv2 supports route summarization. Route summarization can reduce the size of the routing table and improve the efficiency of routing information exchange. The best metric is selected for the summarized route.

- Supernetting route

  If the subnet mask length of a route is smaller than the natural mask length, this route is called supernetting route. For example, 80.0.0.0/6. As 80.0.0.0 is a Class A network address and the natural mask is 8 bits, 80.0.0.0/6 route is a supernetting route.

Note

Only RIPv2 supports supernetting routes.

- Default route

  In the routing table, a route to the destination network 0.0.0.0/0 is called default route.

  The default route can be learned from a neighbor device, or sent to a neighbor device.

- Route redistribution

  For RIP, other types of routes (such as direct routes, static routes, and routes of other routing protocols) are called external routes.

  External routes (excluding the default route) can be redistributed to RIP and advertised to neighbors.

- Route filtering

  Filtering conditions can be configured to limit the routing information exchanged between adjacent routers. Only the routing information that meets filtering conditions can be sent or received.

4. Routing Algorithm

RIP is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.

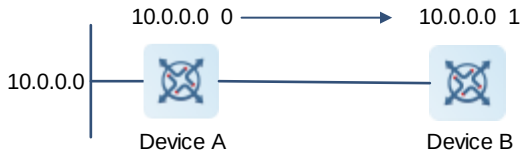
- Distance-vector algorithm

  RIP is a protocol based on the distance-vector algorithm. The distance-vector algorithm treats a route as a vector that consists of the destination network and distance. The device obtains a route from its neighbor and adds the distance vector from itself to the neighbor to the route to form its own route.

  RIP uses the hop count to evaluate the distance to the destination network. By default, the hop count from a device to its directly connected network is 0, the hop count from a device to a network that can be reached through a device is 1, and so on. That is, the metric is equal to the number of devices from the local network to the destination network. To restrict the convergence time, RIP stipulates that the metric must be an integer in the range from 0 to 15. If the metric is equal to or greater than 16, the destination network or host is unreachable. For this reason, RIP cannot be applied to a large-scale network.

  As shown in Figure 1-3, Device A is connected to the network 10.0.0.0. Device B obtains the route (10.0.0.0,0) from Device A and adds the metric 1 to the route to obtain its own route (10.0.0.0,1), and the next hop points to Device A.

Figure 1-3 Diagram of RIP Distance-Vector Algorithm

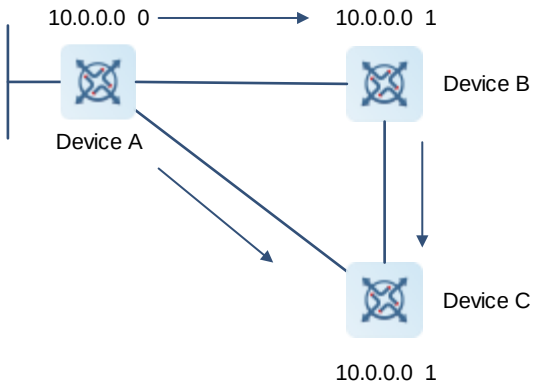


- Selecting the optimum route

RIP selects an optimum route based on the following principle: If multiple routes to the same destination network is available, a device preferentially selects the route with the smallest metric.

As shown in Figure 1-4, Device A is connected to the network 10.0.0.0. Device C obtains the route (10.0.0.0,0) from Device A and the route (10.0.0.0,1) from Device B. Device C will select the route that is obtained from Device A and add metric 1 to this route to form its own route (10.0.0.0,1), and the next hop points to Device A.

Figure 1-4 Diagram of Selecting the Optimum Route



Note

When routes coming from different sources exist on a device, the route with the smaller distance is preferentially selected.

Table 1-1 Default Distance of Routing Protocol

Route Source	Default Distance
Directly-connected network	0
Static route	1
OSPF route	110
IS-IS route	115
RIP route	120
Unreachable route	255

5. Avoiding Route Loops

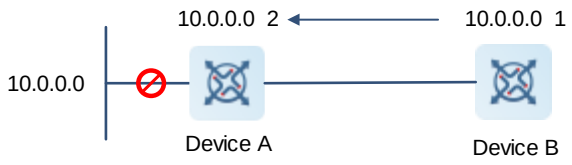
RIP uses functions such as split horizon and poison reverse to avoid route loops.

- Route loop

  A RIP route loop occurs due to inherent defects of the distance-vector algorithm.

  As shown in Figure 1-5, Device A is connected to the network 10.0.0.0, and sends an update packet every 30s. Device B receives the route 10.0.0.0 from Device A every 30s. If Device A is disconnected from 10.0.0.0, the route to 10.0.0.0 will be deleted from the routing table on Device A. Next time, the update packet sent by Device A no longer contains this route. As Device B does not receive an update packet related to 10.0.0.0, Device B determines that the route to 10.0.0.0 is valid within 180s and uses the update packet to send this route to Device A. As the route to 10.0.0.0 does not exist on Device A, the route learned from Device B is added to the routing table. Device B determines that data can reach 10.0.0.0 through Device A, and Device A determines that data can reach 10.0.0.0 through Device B. In this way, a route loop is formed.

Figure 1-5 Diagram of Route Loop



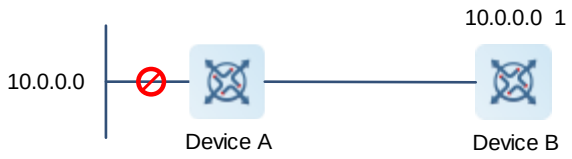
- Split horizon

  Split horizon can prevent route loops. After split horizon is enabled on an interface, a route received on this interface will not be sent out from this interface.

  As shown in Figure 1-6, after split horizon is enabled on the interface between Device A and Device B, Device B will not send the route 10.0.0.0 back to Device A. Device B will learn 180s later that 10.0.0.0 is not reachable.

  On a non broadcast multiple access (NBMA) network, there are multiple neighbors on an interface, and the device communicates with neighbors in unicast form. The routes received by the interface are distinguished by neighbors, and a route learned from a neighbor will not be sent back to this neighbor.

Figure 1-6 Diagram of Split Horizon



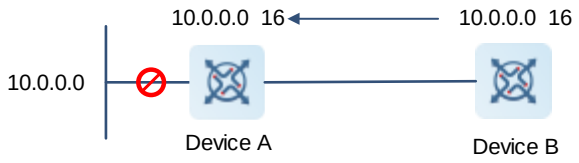
- Poison reverse

  Poison reverse can also prevent route loops. Compared with split horizon, poison reverse is more reliable, but brings more protocol packets, which makes network congestion more severe.

  After poison reverse is enabled on an interface, a route received from this interface will be sent out from this interface again, but the metric of this router will be changed to 16 (unreachable).

As shown in Figure 1-7, after learning the route 10.0.0.0 from Device A, Device B sets the metric of this route to 16 and sends the route back to Device A. After this route becomes invalid, Device B advertises the route 10.0.0.0 (metric = 16) to Device A to accelerate the process of deleting the route from the routing table.

Figure 1-7 Diagram of Poison Reverse



6. Security Measures

RIP uses functions such as authentication and source address verification to ensure protocol security.

- Authentication

  RIPv2 supports authentication, but RIPv1 does not.

  The authentication function is used to prevent unauthorized devices from accessing the RIP routing domain. After authentication is enabled on an interface, the routing information cannot be exchanged between adjacent devices if authentication fails. Authentication is classified into plain text authentication and MD5 authentication:

  Plain text authentication: The configured password is directly added to the packet in the form of plain text, so the security of this authentication mode is low.

  MD5 authentication: The configured password is added to the packet after calculated by MD5 algorithm, so the security of this authentication mode is high.

- Source address verification

  When a RIP-enabled device receives an update packet, it checks whether the source IP address in the packet and the IP address of the inbound interface are in the same network segment. If not, the device drops the packet. Source address verification is used to ensure that RIP routing information is exchanged only between adjacent routing devices.

Note

- On an unnumbered IP interface, source address verification is not performed (not configurable).
- If the triggered updates function is enabled, source address verification is automatically enabled (not configurable).
- If split horizon is disabled, source address verification is automatically enabled (not configurable).

7. Reliability Measures

Use RIP.

Correlate with Bidirectional Forwarding Detection (BFD).

Use fast reroute.

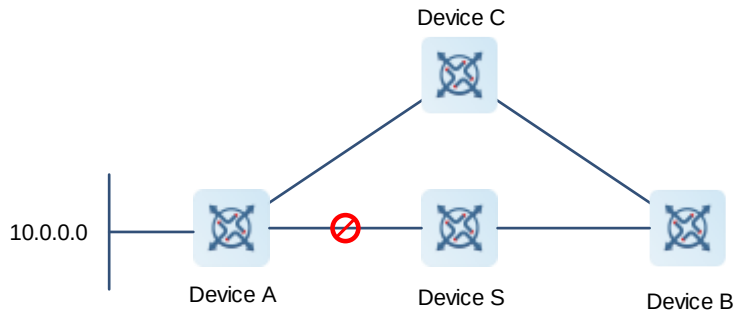
Use graceful restart (GR) and other functions to enhance reliability of the protocol.

- Correlate with BFD.
- Use fast reroute.

  When a link or a device is faulty on the network, packets transmitted through this route will be lost until the route is converged again.

  As shown in Figure 1-8, after the link between Device A and Device S is faulty, Device B may wait for 180s before it can detect the failure of the route (destination network: 10.0.0.0; next hop: Device A). Later, Device B may need to wait for 30s to re-obtain the route (destination network: 10.0.0.0; next hop: Device C) from Device C. Therefore, the traffic is interrupted for 210s.

Figure 1-8 Diagram of Fast Reroute



  Quick detection of a route failure or fast switchover to the standby route helps shorten the traffic interruption time.

  - A BFD session can be set up between Device A and Device B, and correlated with RIP. BFD can quickly test the connectivity between adjacent devices. Once a link is faulty, RIP can detect the route failure within 1s.
  - The fast reroute function can be enabled. A backup route (destination network: 10.0.0.0; next hop: Device C) can be configured on Device B in advance. Once RIP detects a route failure, the backup route is immediately enabled.

- GR

  GR ensures uninterrupted data transmission when the protocol is restarted. If RIP is restarted on a GR-enabled device, the forwarding table before restart will be retained and a request packet will be sent to the neighbor so that the route can be learned again. During the GR period, RIP completes re-convergence of the route. After the GR period expires, RIP updates the forwarding entry and advertises the routing table to the neighbor.

8. Multiple VPN Instances

Multiple VPN instances may exist on a device.

RIP supports multiple instances. You can enable the RIP process in VPN routing and forwarding (VRF) address family mode to run RIP on VPN instances. One VRF address family is mapped to one VPN instance.

VPN instances cannot be distinguished from each other when you perform RIP operations using SNMP. You must bind the management information base (MIB) of RIP with a VPN instance before the SNMP operations take effect on the VPN instance.

1.1.3 Protocols and Standards

- RFC 1058: Routing Information Protocol
- RFC 2453: RIP Version 2

1.2 Configuration Task Summary

The RIP configuration includes the following tasks:

(1) Configuring Basic Features

a Enabling RIP Process

b Configuring Association with the Local Network

c (Optional) Configuring RIP Version

d (Optional) Configuring Split Horizon

e (Optional) Configuring a Passive Interface

f (Optional) Enabling Triggered Updates

(2) (Optional) Enabling RIP Route Summarization

a Configuring to Enable Automatic Route Summarization Function

b Configuring RIP Route Summarization on an Interface

(3) (Optional) Configuring RIP Route Filtering Rules The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Filter the Received RIP Routing Information
- Configuring to Filter the Sent RIP Routing Information

(4) (Optional) Configuring to Adjust RIP Routing The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Modify the Management Distance of a RIP Route
- Configuring to Increase the Metric of a Received or Sent RIP Route Metric
- Configuring the Default Metric of an External Route Redistributed to RIP

(5) (Optional) Modifying Timers The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Modify the Update Timer, Invalid Timer, Flush Timer, and Holddown Timer of a RIP Route
- Configuring the Sending Delay Between RIP Route Update Packets

(6) (Optional) Configuring RIP Route Distribution The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Advertise a Default Route to Neighbors
- Configuring to Advertise a Default Route to Neighbors on an Interface
- Configuring Route Redistribution

(7) (Optional) Controlling Interaction of RIP Packets The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Send Unicast RIP Route Update Packets
- Configuring to Send Broadcast RIPv2 Packets on an Interface
- Configuring to Allow an Interface to Receive RIP Packets
- Configuring to Allow an Interface to Send RIP Packets
- Configuring to Allow an Interface to Send RIP Packets of a Specified Version
- Configuring to Allow an Interface to Receive RIP Packets of a Specified Version

(8) (Optional) Configuring to Enable RIPv2 Authentication

a Configuring RIP Authentication Mode

b Configuring a Key Chain for Authentication

c Configuring a Key Chain for RIP Plain Text Authentication

(9) (Optional) Configuring BFD Correlation with RIP

- Configuring BFD Correlation with RIP Globally
- Configuring BFD Correlation with RIP on an Interface

(10) (Optional) Configuring to Enable RIP Fast Reroute

(11) (Optional) Enabling GR

(12) (Optional) Configuring to Enable RIP Supernetting Routes

(13) (Optional) Configuring RIP to Enable Multiple VRF Instances

a Configuring a VRF Instance

b Configuring to Bind a RIP MIB with a VRF Instance

(14) (Optional) Configuring a Super VLAN to Enable RIP

(15) (Optional) Enabling Source Address Verification

1.3 Configuring Basic Features

1.3.1 Overview

Build a RIP routing domain on the network. Devices in the domain obtain routes to a remote network through RIP.

1.3.2 Restrictions and Guidelines

- IPv4 addresses must be configured.
- IPv4 unicast routes must be enabled.

1.3.3 Configuration Tasks

The basic function configuration of RIP includes the following tasks:

(1) Enabling RIP Process

(2) Configuring Association with the Local Network

(3) (Optional) Configuring RIP Version

(4) (Optional) Configuring Split Horizon

(5) (Optional) Configuring a Passive Interface

(6) (Optional) Enabling Triggered Updates

1.3.4 Enabling RIP Process

1. Overview

This command is used to create a RIP routing process and enter the RIP routing process configuration mode.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable a RIP routing process and enter the RIP routing process configuration mode.

router rip

The RIP routing process is disabled by default.

1.3.5 Configuring Association with the Local Network

1. Overview

To add an interface to the RIP domain, you need to first advertise the interface network in the RIP process.

2. Restrictions and Guidelines

- RIP can run and learn direct routes and RIP packets can be exchanged only on an interface covered by the **network**.
- If **network** 0.0.0.0 255.255.255.255 is configured, all interfaces are covered.
- If the *wildcard* parameter is not configured, the classful address range is used by default, that is, the interfaces whose addresses fall into the classful address range participate in RIP operations.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure association with the local network.

network *network-number* [*wildcard*]

1.3.6 Configuring RIP Version

1. Overview

You can run this command to define the versions of RIP packets sent or received on all interfaces. This command takes effect on the entire device.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure a RIP version.

version { **1** | **2** }

By default, route update packets of RIPv1 and RIPv2 can be received, but only route update packets of RIPv1 are sent.

1.3.7 Configuring Split Horizon

1. Overview

This function prevents route loop. After split horizon is enabled on an interface, a route received on this interface will not be sent out from this interface.

2. Restrictions and Guidelines

After poison reverse is enabled, split horizon is automatically disabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable split horizon.

ip rip split-horizon [**poisoned-reverse**]

By default, the split horizon function is enabled, but poison reverse is disabled.

1.3.8 Configuring a Passive Interface

1. Overview

The interface set to a passive interface suppresses RIP update packets. A passive interface defines the boundary of RIP routing domain to avoid unwanted flooding of RIP packets. If the interface connection device does not run the RIP routing protocol (such as a PC and a device running other routing protocols), you are advised to configure this interface as a passive interface.

2. Restrictions and Guidelines

You are advised to set all interfaces to passive interfaces in RIP routing process configuration mode, and then enter the device interconnection interface in the specific domain to disable the passive interface function.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure passive interfaces.

passive-interface { **default** | *interface-type interface-number* }

The passive-interface function is disabled by default.

1.3.9 Enabling Triggered Updates

1. Overview

Enable the RIP triggered updates function, after which RIP does not periodically send route update packets. This function can quickly obtain network changes, avoid route loops, and improve the convergence speed.

2. Restrictions and Guidelines

- The basic functions of RIP must be configured.
- It is recommended that split horizon with poison reverse be enabled; otherwise, invalid routing information may exist.
- This function cannot be enabled together with the function of correlating RIP with BFD.
- Ensure that the triggered updates function is enabled on every router on the same link; otherwise, the routing information cannot be exchanged properly.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable triggered updates.

ip rip triggered [**retransmit-timer** *timer* | **retransmit-count** *count*]

The RIP triggered updates function is disabled by default.

1.4 Enabling RIP Route Summarization

1.4.1 Overview

This function can reduce the size of the routing table, improve the routing efficiency, avoid route flapping to some extent, and improve scalability and effectiveness of the network.

1.4.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- The range of supernetting routes is larger than that of the classful network. Therefore, the automatic route summarization function is invalid for supernetting routes.
- RIPv1 performs automatic route summarization by default. If the detailed routes should be advertised, you must set the RIP version to RIPv2.

1.4.3 Configuration Tasks

The configuration for enabling RIP route summarization includes the following tasks:

(1) Configuring to Enable Automatic Route Summarization Function

(2) Configuring RIP Route Summarization on an Interface

1.4.4 Configuring to Enable Automatic Route Summarization Function

1. Overview

This function can be configured to reduce the size of the routing table, improve the routing efficiency, avoid route flapping to some extent, and improve scalability and effectiveness of the network.

2. Restrictions and Guidelines

- Route summarization is enabled by default for RIPv1 and RIPv2.
- You can disable automatic route summarization only when RIPv2 is configured.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Enable the automatic route summarization function.

auto-summary

The automatic summarization function of RIP routes is enabled by default.

1.4.5 Configuring RIP Route Summarization on an Interface

1. Overview

This function is used to manually summarize an address or a subnet on a specified interface.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure RIP route summarization on an interface.

ip rip summary-address *ipv4-address mask*

By default, RIP route summarization is not configured on an interface.

1.5 Configuring RIP Route Filtering Rules

1.5.1 Overview

Routes that do not meet filtering criteria cannot be loaded to the routing table, or advertised to neighbors. In this way, users within the network can be prevented from accessing specified destination networks.

1.5.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- In regard to the filtering rules of sent routes, you must configure route redistribution first, and then filter the redistributed routes.

1.5.3 Configuration Tasks

The configuration of RIP route filtering rules includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Filter the Received RIP Routing Information
- Configuring to Filter the Sent RIP Routing Information

1.5.4 Configuring to Filter the Received RIP Routing Information

1. Overview

You can configure the route distribution control list to refuse to receive some specified routes. If no interface is specified, the route update packets received on all interfaces will be filtered.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ACL or prefix list. Please configure only one task.

- Configure an ACL.

  access-list *acl-number* { **deny** | **permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *tm-range-name*] [**log**]

- Configure a prefix list.

  ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

(4) Enter the RIP routing process configuration mode.

router rip

(5) Filter the received RIP routing information.

distribute-list { [*acl-number* | *acl-name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

There is no inbound distribution list by default.

1.5.5 Configuring to Filter the Sent RIP Routing Information

1. Overview

You can configure the route distribution control list to prohibit distributing some specified routes. If no interface is specified, the route update packets sent to all interfaces will be filtered.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure an ACL or prefix list. Please configure only one task.

- Configure an ACL.

  access-list *acl-number* { **deny** | **permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *tm-range-name*] [**log**]

- Configure a prefix list.

  ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

(5) Filter the sent RIP routing information.

distribute-list { [*acl-name* | *acl-number*] | **prefix** *prefix-list-name* } **out** [*interface-type interface-number* | **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

There is no outbound distribution list by default.

1.6 Configuring to Adjust RIP Routing

1.6.1 Overview

This function can be used to change a RIP route so that the traffic passes through specified nodes or bypasses specified nodes. Change the sequence that a device selects various types of routes so as to change the priorities of RIP routes.

1.6.2 Restrictions and Guidelines

The basic functions of RIP must be configured.

1.6.3 Configuration Tasks

The configuration of RIP routing adjustment includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Modify the Management Distance of a RIP Route
- Configuring to Increase the Metric of a Received or Sent RIP Route Metric
- Configuring the Default Metric of an External Route Redistributed to RIP

1.6.4 Configuring to Modify the Management Distance of a RIP Route

1. Overview

This function is used to set the management distance of RIP routes and change the priority of a device in routing.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to modify the management distance of a RIP route.

distance *distance* [*ipv4-address wildcard*]

The management distance is **120** by default.

1.6.5 Configuring to Increase the Metric of a Received or Sent RIP Route

1. Overview

You can use this function to increase the metric of a received or sent RIP route. If an interface is specified, the configuration takes effect only on the specified interface; otherwise, the configuration takes effect globally.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to increase the metric of a received or sent RIP route.

offset-list { *acl-number* | *acl-name* } { **in** | **out** } *offset* [*interface-type interface-number*]

The metric of a received or sent RIP route is not increased by default.

1.6.6 Configuring the Default Metric of an External Route Redistributed to RIP

1. Overview

The default metric of a redistributed route is 1. If you want to preferably select an internal RIP route on some networks, just increase the default metric.

2. Restrictions and Guidelines

This function needs to be used together with the routing protocol redistribution function.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure the default metric of an external route redistributed to RIP.

default-metric *metric-value*

By default, the metric of a redistributed route is 1.

1.7 Modifying Timers

1.7.1 Overview

This function can be used to change the durations of RIP timers to accelerate or slow down change to the protocol state or occurrence of an event.

1.7.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- Modifying the protocol control parameters may result in protocol running failures. Therefore, you are advised not to modify the timers.

1.7.3 Configuration Tasks

The configuration of RIP timer modification includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Modify the Update Timer, Invalid Timer, Flush Timer, and Holddown Timer of a RIP Route
- Configuring the Sending Delay Between RIP Route Update Packets

1.7.4 Configuring to Modify the Update Timer, Invalid Timer, Flush Timer, and Holddown Timer of a RIP Route

1. Overview

By adjusting the timers, you can reduce the convergence time and fault rectification time of the routing protocol.

2. Restrictions and Guidelines

For devices connected to the same network, the values of RIP timers must be consistent. Generally, you are not advised to modify the RIP timers unless otherwise required.

Setting timers to small values on a low-speed link brings risks because a lot of update packets consume the bandwidth. You can set timers to small values generally on the Ethernet or a link of 2 Mbps (or above) to reduce the convergence time of network routes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to modify the update timer, invalid timer, flush timer, and holddown timer of a RIP route.

timers basic *update invalid flush* [**holddown** *holddown*]

By default, the update timer is 30s, the invalid timer is 180s, the flush timer is 120s, and the holddown timer is 0s.

1.7.5 Configuring the Sending Delay Between RIP Route Update Packets

1. Overview

A RIP route update packet is 512 bytes long and can contain 25 routes. If the number of routes to be updated exceeds 25, more than one update packet will be sent as fast as possible. When a high-speed device sends a lot of update packets to a low-speed device, the low-speed device may fail to process all update packets in time, causing

loss of routing information. This function can be used to increase the sending delay between packets on a high-speed device so that a low-speed device can receive and process all the update packets.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the sending delay between RIP route update packets.

output-delay *delay*

The sending delay between update packets is 0 by default.

1.8 Configuring RIP Route Distribution

1.8.1 Overview

In the RIP domain, you can introduce a unicast route or default route of another AS so that the unicast routing service to this AS can be provided for users in the RIP domain.

To enable a RIP routing domain to communicate with other ASs, a default route to another AS can be injected into the RIP routing domain, or the route of another AS can be redistributed to the RIP routing domain.

1.8.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- Route redistribution cannot introduce default routes of other protocols to the RIP routing domain.

1.8.3 Configuration Tasks

The configuration of RIP route distribution includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Advertise a Default Route to Neighbors
- Configuring to Advertise a Default Route to Neighbors on an Interface
- Configuring Route Redistribution

1.8.4 Configuring to Advertise a Default Route to Neighbors

1. Overview

RIP will not advertise the default route in the routing table to neighbors by default. If you need to advertise the default route to the neighbors, use this function.

2. Restrictions and Guidelines

You still need to run the **default-information originate** command to introduce the default route generated by **ip default-network** to RIP.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Advertise the default route to neighbors.

default-information originate [**always**] [**metric** *metric-value*] [**route-map** *route-map-name*]

1.8.5 Configuring to Advertise a Default Route to Neighbors on an Interface

1. Overview

If a default route needs to be advertised to some neighbors only, the default route to be advertised can be configured on the related interfaces, and RIP will advertise it to neighbors on the configured interfaces only.

2. Restrictions and Guidelines

- If you configure the **ip rip default-information** command for the interface, and the **default-information originate** command for the RIP process at the same time, only the default route configured for the interface is advertised.
- So far as the **ip rip default-information** command is configured for an interface, RIP does not learn the default route advertised by the neighbor.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Advertise the default route to neighbors on an interface.

ip rip default-information { **only** | **originate** } [**metric** *metric-value*]

By default, default route advertisement is disabled on an interface.

1.8.6 Configuring Route Redistribution

1. Overview

The function redistributes the routes of other protocols to the RIP domain to implement internetworking between the RIP domain and other routing domains.

2. Restrictions and Guidelines

- If the **level** parameter is not carried when IS-IS route redistribution is configured, only level-2 routes can be redistributed by default. If the **level** parameter is carried during initial configuration of redistribution, the routes configured with the **level** parameter can be redistributed. If both **level 1** and **level 2** are configured, the two levels are combined and saved as **level-1-2**.
- If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be distributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can run the **no** form of the command to restore the default value of **match**.
- The configuration rules for the **no** form of the **redistribute** command are as follows:
  - If some parameters are specified in the **no** form of this command, default values of these parameters will be restored.
  - If no parameter is specified in the **no** form of this command, the entire command will be deleted.
- For example, if **redistribute isis 112 level-2** is configured, you can run the **no redistribute isis 112 level-2** command to restore the default value of level-2. As **level-2** itself is the default value of the parameter, the configuration saved is still **redistribute isis 112 level-2** after the preceding **no** form of the command is executed. To delete the entire command, run the **no redistribute isis 112** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Redistribute routes and advertise external routes to neighbors.

redistribute { **bgp** | **connected** | **isis** [*area-tag*] [**level-1** | **level-1-2** | **level-2**] | **ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **static** } [**metric** *metric-value* | **route-map** *route-map-name*] *

The redistribution function is not configured by default.

If OSPF redistribution is configured, the routes of all sub-types of the instance will be redistributed.

If IS-IS redistribution is configured, redistribute the level-2 routes of the IS-IS process.

In other cases, all routes of this type are redistributed.

1.9 Controlling Interaction of RIP Packets

1.9.1 Overview

This function can be used to change the default running mechanism of RIP through configuration and control the interaction mode of RIP packets.

The following interaction modes of RIP packets can be implemented:

Allowing or prohibiting the sending of unicast RIP packets to a specified neighbor on an interface

Allowing or prohibiting the sending of unicast RIPv2 packets instead of broadcast packets to a specified neighbor on an interface

Allowing or prohibiting the receiving of RIP packets on an interface

Allowing or prohibiting the sending of RIP packets on an interface

Allowing or prohibiting the receiving of RIP packets of a specified version on an interface

Allowing or prohibiting the sending of RIP packets of a specified version on an interface

1.9.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- On an interface connecting to a neighbor device, the configured version of sent RIP packets must be the same as the version of received RIP packets.

1.9.3 Configuration Tasks

The configuration of RIP packet interaction includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Send Unicast RIP Route Update Packets
- Configuring to Send Broadcast RIPv2 Packets on an Interface
- Configuring to Allow an Interface to Receive RIP Packets
- Configuring to Allow an Interface to Send RIP Packets
- Configuring to Allow an Interface to Send RIP Packets of a Specified Version
- Configuring to Allow an Interface to Receive RIP Packets of a Specified Version

1.9.4 Configuring to Send Unicast RIP Route Update Packets

1. Overview

This function can be configured if you hope that only some of devices connected to an interface can receive the updated routing information or when RIP is used for a non-broadcast network.

2. Restrictions and Guidelines

Generally, you can first enable the passive interface function in routing process configuration mode, and then specify the neighbors that can receive the routing information. This command does not affect the receiving of RIP packets. After an interface is configured as a passive interface, the interface does not send a request packet even after the device is restarted.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to send unicast RIP route update packets to a specified neighbor.

neighbor *ipv4-address*

No RIP neighbor is configured by default.

1.9.5 Configuring to Send Broadcast RIPv2 Packets on an Interface

1. Overview

This function can be configured if the neighbor device does not support receiving of multicast RIPv2 packets.

2. Restrictions and Guidelines

- The default behavior depends on the configuration of the **version** command.
- The configuration result of this command can overwrite the default configuration of the **version** command.
- This command affects the behavior of sending RIP packets on the current interface, and the interface is allowed to send RIPv1 and RIPv2 packets simultaneously.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to send broadcast RIPv2 packets on an interface.

ip rip v2-broadcast

By default, RIPv2 packets are multicast on an interface.

1.9.6 Configuring to Allow an Interface to Receive RIP Packets

1. Overview

If you want to prevent an interface from receiving RIP packets, you can enable this function.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to allow an interface to receive RIP packets.

ip rip receive enable

By default, an interface can receive RIP packets normally.

1.9.7 Configuring to Allow an Interface to Send RIP Packets

1. Overview

If you want to prevent an interface from sending RIP packets, you can disable this function.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to allow an interface to send RIP packets.

ip rip send enable

By default, the RIP packet sending function is enabled on an interface.

1.9.8 Configuring to Allow an Interface to Send RIP Packets of a Specified Version

1. Overview

To be compatible with the RIP version running on the peer device, use this function to change the version of RIP packets sent by the interface.

2. Restrictions and Guidelines

- The default behavior depends on the configuration of the **version** command.
- The configuration result of this command can overwrite the default configuration of the **version** command.
- This command affects the behavior of sending RIP packets on the current interface, and the interface is allowed to send RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets depends on the configuration of the **version** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to allow an interface to send RIP packets of a specified version.

ip rip send version [**1**] [**2**]

By default, the default behavior depends on the configuration of the **version** command.

1.9.9 Configuring to Allow an Interface to Receive RIP Packets of a Specified Version

1. Overview

To be compatible with the RIP version running on the peer device, use this function to change the version of RIP packets that can be received by the interface.

2. Restrictions and Guidelines

- The default behavior depends on the configuration of the **version** command.
- The configuration result of this command can overwrite the default configuration of the **version** command.
- This command affects the behavior of receiving RIP packets on the current interface, and the interface is allowed to receive RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the

behavior of receiving RIP packets depends on the configuration of the **version** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to allow an interface to receive RIP packets of a specified version.

ip rip receive version [**1**] [**2**]

By default, the default behavior depends on the configuration of the **version** command.

1.10 Configuring to Enable RIPv2 Authentication

1.10.1 Overview

This function prevents learning unauthenticated and invalid routes and advertising valid routes to unauthenticated devices, ensuring stability of the routing system, and protecting the system against intrusions.

1.10.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- Only RIPv2 supports authentication of RIP packets, and RIPv1 does not.

1.10.3 Configuration Tasks

The configuration for enabling RIPv2 authentication includes the following tasks:

(1) Configuring RIP Authentication Mode

(2) Configuring a Key Chain for Authentication

(3) Configuring a Key Chain for RIP Plain Text Authentication

1.10.4 Configuring RIP Authentication Mode

1. Overview

RIPv2 supports plain text authentication and cipher text authentication, and ensures secure transmission of RIP packets.

2. Restrictions and Guidelines

- For all devices that need to directly exchange the RIP routing information, the RIP authentication mode of these devices must be the same.

- Cipher text authentication is recommended because the plain text password is saved in the configuration file and the security is low.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the RIP authentication mode.

ip rip authentication mode { **text** | **md5** }

Plain text authentication mode is used by default.

1.10.5 Configuring a Key Chain for Authentication

1. Overview

A key chain can be used to change the key dynamically to improve the security.

2. Restrictions and Guidelines

- The specified key chain must be defined using the **key chain** command in global configuration mode in advance.
- If this command and the **ip rip authentication mode md5** command are configured, MD5 mode authentication is adopted. If the **ip rip authentication mode** command is not configured, authentication is performed according to the authentication mode specified by the configured **key chain**. MD5 authentication and SM3 authentication are supported at present.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a key chain for authentication.

ip rip authentication key-chain *name-of-keychain*

No key chain is set by default.

1.10.6 Configuring a Key Chain for RIP Plain Text Authentication

1. Overview

This function uses a string to implement plain text encryption and improve the security of RIP packet transmission.

2. Restrictions and Guidelines

- This function takes effect only in plain text authentication mode.
- Encrypted strings can be displayed in plain text or cipher text. Cipher text is recommended.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable RIP plain text authentication and configure a key chain.

ip rip authentication text-password [**0** | **7**] *password-string*

No character string of plain text authentication is set by default.

1.11 Configuring BFD Correlation with RIP

1.11.1 Overview

Once a link fails, RIP can quickly detect the failure of the route. This function helps shorten the traffic interruption time.

1.11.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- The BFD correlation configured in interface configuration mode takes precedence over the global configuration.

1.11.3 Configuration Tasks

The configuration for enabling BFD correlation with RIP includes the following tasks:

- Configuring BFD Correlation with RIP Globally
- Configuring BFD Correlation with RIP on an Interface

1.11.4 Configuring BFD Correlation with RIP Globally

1. Overview

This function enables BFD correlation with RIP globally. Once a link fails, RIP can quickly detect the failure of the route, which helps shorten the traffic interruption time.

After BFD is enabled on RIP, a BFD session will be set up for the RIP routing information source (that is, the source address of RIP route update packets). Once the BFD neighbor fails, the corresponding RIP route directly enters the invalid state and is not forwarded.

2. Restrictions and Guidelines

The BFD configured on an interface takes precedence over that configured in process configuration mode.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to enable BFD correlation with RIP globally.

bfd all-interfaces

The BFD function is disabled by default.

1.11.5 Configuring BFD Correlation with RIP on an Interface

1. Overview

This function enables BFD correlation with RIP on an interface. Once an interface link fails, RIP can quickly detect the failure of the route, which helps shorten the traffic interruption time.

2. Restrictions and Guidelines

- By default, the BFD configuration is subject to that configured in RIP process configuration mode.
- This configuration must be performed if you need to enable or disable BFD correlation on a specified interface.
- The BFD configured on an interface takes precedence over that configured in RIP process configuration mode.
- According to the actual environment, you can select to enable BFD on the specified interface, or enable BFD globally in RIP process, or disable BFD on the specified interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure BFD correlation with RIP on an interface.

ip rip bfd [**disable**]

By default, BFD link detection on an interface is disabled by default.

1.12 Configuring to Enable RIP Fast Reroute

1.12.1 Overview

Once RIP detects a route failure, the router immediately switches to the second-best route. This configuration helps shorten the traffic interruption time.

1.12.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- The route map and the backup next hop must be configured.
- To accelerate convergence, set **carrier-delay** of the interface to **0** and enable BFD correlation with RIP.

1.12.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a routing policy.

route-map *route-map-name* [{ **permit** | **deny** } *sequence*]

(4) Run this command to configure the interface-based matching rule.

match interface { *interface-type interface-number* }&<1-n>

(5) Return to the global configuration mode.

exit

(6) Enter the RIP routing process configuration mode.

router rip

(7) Enable fast reroute.

fast-reroute route-map *route-map-name*

The fast reroute function is disabled by default.

1.13 Enabling GR

1.13.1 Overview

The GR period is the maximum time from restart of the RIP process to completion of the restart. During this period, RIP performs route recovery and the forwarding table remains unchanged. After the restart period expires, RIP exits the GR state and performs common RIP operations.

1.13.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- The GR period is at least twice the RIP route update period.

1.13.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Enable GR.

graceful-restart [**grace-period** *grace-period*]

The GR function is enabled by default.

1.14 Configuring to Enable RIP Supernetting Routes

1.14.1 Overview

This function is used to allow RIP to send RIP supernetting routes on a specified interface. The concept of supernetting is similar to that of subnet. Subnet means dividing a large network segment into several small network segments, while supernetting means aggregating some small network segments into a large network segment. The number of network address bits allowed by supernetting is larger than that allowed by a classful network.

1.14.2 Restrictions and Guidelines

The basic functions of RIP must be configured.

1.14.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable supernetting routes.

ip rip send supernet-routes

By default, the supernetting route sending function is enabled on an interface.

1.15 Configuring RIP to Enable Multiple VRF Instances

1.15.1 Overview

This function is used to run RIP on VPN instances.

1.15.2 Restrictions and Guidelines

The RIP basic functions (with the VRF parameter) must be configured.

1.15.3 Configuration Tasks

The RIP configuration for enabling multiple VRF instances includes the following tasks:

(1) Configuring a VRF Instance

(2) Configuring to Bind a RIP MIB with a VRF Instance

1.15.4 Configuring a VRF Instance

1. Overview

This function is used to create a VRF instance.

2. Restrictions and Guidelines

This function must be configured if you need to configure multiple RIP instances and associate these RIP instances with VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Create a VRF instance and enter the IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

The address family of RIP is disabled by default.

(5) Exit the IPv4 VRF address family.

exit-address-family

1.15.5 Configuring to Bind a RIP MIB with a VRF Instance

1. Overview

If multiple RIP instances have been configured, this function can be used to manage non-default RIP instances using the MIB.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Configure to bind a RIP MIB with a VRF instance.

enable mib-binding

By default, the MIB is bound with the RIP instance of the default VRF.

1.16 Configuring a Super VLAN to Enable RIP

1.16.1 Overview

This function is used to run RIP on a super VLAN. A super VLAN is also called VLAN aggregation. Multiple sub VLANs are associated with one super VLAN. All sub VLANs share the SVI interface of the super VLAN and use it as the gateway of Layer-3 communication to save IP resources.

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when RIP multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIP multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing protocol flapping.

In most scenarios, the RIP function does not need to be enabled on a super VLAN, and it is disabled by default. However, in some scenarios, the RIP function must be run on the super VLAN, but packets need to be sent to only one sub VLAN. In this case, you can decide to send multicast packets to a certain sub VLAN or to all sub VLANs as

actually needed. You can run this command to specify a particular sub VLAN. You must be cautious when configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

1.16.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- The designated sub VLAN must be connected to neighbors.

1.16.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the inbound interface configuration mode.

interface vlan *vlan-id*

(4) Configure to enable RIP.

ip rip subvlan [**all |** *vlan-id*]

By default, RIP is disabled on a super VLAN.

1.17 Enabling Source Address Verification

1.17.1 Overview

You can run the command to validate the source address of a RIP route update packet. The purpose is to ensure that the RIP routing process receives only the route update packets coming from the same IP subnet neighbor.

1.17.2 Restrictions and Guidelines

- The basic functions of RIP must be configured.
- After split horizon is disabled on an interface, the RIP routing process will perform source address validation on the update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.
- For an interface not configured with an IP address, the RIP routing process does not perform source address validation for the update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.

1.17.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing process configuration mode.

router rip

(4) Enables source address verification.

validate-update-source

The source address validation function for update packets is enabled by default.

1.18 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2 RIP Monitoring

Command	Purpose
show ip rip [**vrf** *vrf-name*]	Displays the basic information about a RIP process.
show ip rip database [**vrf** *vrf-name*] [*network-number network-mask*] [**count**]	Displays the RIP routing table.
show ip rip external [**bgp** | **connected** | **isis** [*process-id*] | **ospf** *process-id* | **static**] [**vrf** *vrf-name*]	Displays information about external routes redistributed by RIP.
show ip rip interface [**vrf** *vrf-name*] [*interface-type interface-number*]	Displays the RIP interface information.
show ip rip peer [*ipv4-address*] [**vrf** *vrf-name*]	Displays the RIP neighbor information.
debug ip rip event	Debugs events that occur when the RIP process is running.
debug ip rip nsm	Debugs interaction with the NSM process.
debug ip rip packet [**interface** *interface-type interface-number* | **recv** | **send**]	Debugs the sent and received packets.
debug ip rip restart	Debugs the RIP GR process.

Command	Purpose
debug ip rip route	Debugs the route changes of the RIP process.

1.19 Configuration Examples

1.19.1 Building a RIP Routing Domain

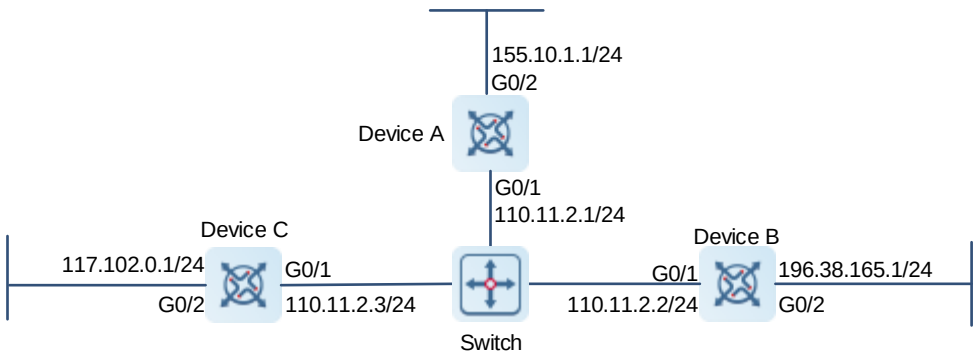
1. Requirements

Device A, Device B, and Device C implement interworking through the RIPv2 routing protocol.

To save the device performance, all interfaces of the three devices are configured as passive interfaces by default, and passive interface is disabled only for the interfaces directly connected to RIP neighbors.

2. Topology

Figure 1-9 Topology for Building a RIP Routing Domain



3. Notes

- Configure interface IP addresses for all the devices.
- Configure the RIP basic functions for all the devices.

4. Procedure

(1) Configure an IP address for each interface and start the unicast routing protocol.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# no switchport
```

```
Device A(config-if-GigabitEthernet 0/1)# ip address 110.11.2.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface GigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# no switchport
Device A(config-if-GigabitEthernet 0/2)# ip address 155.10.1.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/2)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# no switchport
Device B(config-if-GigabitEthernet 0/1)# ip address 110.11.2.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# no switchport
Device B(config-if-GigabitEthernet 0/2)# ip address 196.38.165.1 255.255.255.0
Device B(config-if-GigabitEthernet 0/2)# exit
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# no switchport
Device C(config-if-GigabitEthernet 0/1)# ip address 110.11.2.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface GigabitEthernet 0/2
Device C(config-if-GigabitEthernet 0/2)# no switchport
Device C(config-if-GigabitEthernet 0/2)# ip address 117.102.0.1 255.255.0.0
Device C(config-if-GigabitEthernet 0/2)# exit
```

(2) Configure the RIP basic functions for the devices. Except the RIP neighbor interface, configure the other interfaces as passive interfaces.

Configure Device A.

```
Device A(config)# router rip
Device A(config-router)# version 2
Device A(config-router)# network 0.0.0.0 255.255.255.255
Device A(config-router)# passive-interface default
Device A(config-router)# no passive-interface GigabitEthernet 0/1
```

Configure Device B.

```
Device B(config)# router rip
Device B(config-router)# version 2
Device B(config-router)# network 0.0.0.0 255.255.255.255
```

```
Device B(config-router)# passive-interface default
Device B(config-router)# no passive-interface GigabitEthernet 0/1
```

Configure Device C.

```
Device C(config)# router rip
Device C(config-router)# version 2
Device C(config-router)# no auto-summary
Device C(config-router)# network 0.0.0.0 255.255.255.255
Device C(config-router)# passive-interface default
Device C(config-router)# no passive-interface GigabitEthernet 0/1
```

5. Verification

Check the IP routing tables on Device A, Device B, and Device C. Verify that RIP has learned the routes to remote networks.

- Device A

```
Device A# show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C   110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C   110.11.2.1/32 is local host.
R   117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
C   155.10.1.0/24 is directly connected, GigabitEthernet 0/2
C   155.10.1.1/32 is local host.
C   192.168.217.0/24 is directly connected, VLAN 1
C   192.168.217.233/32 is local host.
R   196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
```

- Device B

```
Device B# show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
```

```
Gateway of last resort is no set
C   110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C   110.11.2.2/32 is local host.
R   155.10.0.0/16 [120/1] via 110.11.2.1, 00:15:21, GigabitEthernet 0/1
C   196.38.165.0/24 is directly connected, GigabitEthernet 0/2
C   196.38.165.1/32 is local host.
R   117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
```

- Device C

```
Device C# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C   110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C   110.11.2.3/32 is local host.
C   117.102.0.0/16 is directly connected, GigabitEthernet 0/2
C   117.102.0.1/32 is local host.
R   155.10.0.0/16 [120/1] via 110.11.2.1, 00:20:55, GigabitEthernet 0/1
R   196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
```

6. Configuration Files

- Device A configuration file.

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 110.11.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 155.10.1.1 255.255.255.0
!
router rip
 version 2
 passive-interface default
 no passive-interface GigabitEthernet 0/1
 network 0.0.0.0
!
```

- Device B configuration file.

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 110.11.2.2 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 196.38.165.1 255.255.255.0
!
router rip
 version 2
 passive-interface default
 no passive-interface GigabitEthernet 0/1
 network 0.0.0.0
!
```

- Device C configuration file.

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 110.11.2.3 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 117.102.0.1 255.255.255.0
!
router rip
 version 2
 no auto-summary
 passive-interface default
 no passive-interface GigabitEthernet 0/1
 network 0.0.0.0
!
```

7. Common Errors

- The IPv4 address is not configured on an interface.
- The RIP version is not defined on a device, or the RIP version No. on the device is different from that on other devices.
- The address range configured using the **network** command does not cover a specific interface.
- The IP address comparison bit parameter in the **network** command is not correctly configured. Value 0 indicates accurate matching, and 1 indicates that no comparison is performed.

- The interface used for interworking between devices is configured as a passive interface.

1.19.2 Configuring RIP to Prevent Route Loop

1. Requirements

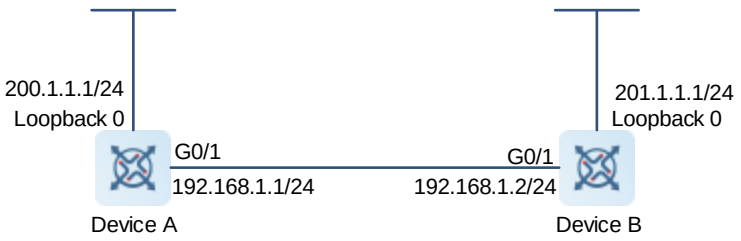
Device A, Device B, and Device C implement interworking through the RIP routing protocol.

To avoid route loop, you need to configure split horizon with poison reverse and triggered updates.

To improve reliability, enable GR, and then enable BFD on the connection interface of Device A and Device B.

2. Topology

Figure 1-10 Topology for Enabling Triggered Updates



3. Notes

(1) Configure interface IP addresses for all devices (omitted).

(2) Configure the RIP basic functions for all the devices.

(3) Enable RIP triggered updates and poison reverse on Device A and Device B.

4. Procedure

(1) Configure interface IP addresses for all devices (omitted).

(2) Enable the RIP process of the device and advertise the network information of each interface.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# router rip
Device A(config-router)# network 192.168.1.0
Device A(config-router)# network 200.1.1.0
Device A(config-router)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# router rip
```

```
Device B(config-router)# network 192.168.1.0
Device B(config-router)# network 201.1.1.0
Device B(config-router)# exit
```

(3) Enable RIP poison reverse and triggered updates.

Configure Device A.

```
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip rip triggered
Device A(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse
```

Configure Device B.

```
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip rip triggered
Device B(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse
```

5. Verification

Check the RIP databases of Device A and Device B, and verify that the corresponding route attributes are permanent.

- Device A

```
Device A# show ip rip database
201.1.1.0/24   auto-summary
201.1.1.0/24
[1] via 192.168.12.2 GigabitEthernet 0/1  06:25   permanent
```

- Device B

```
Device B# show ip rip database
200.1.1.0/24   auto-summary
200.1.1.0/24
   [1] via 192.168.12.1 GigabitEthernet 0/1  06:25   permanent
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
ip rip split-horizon poisoned-reverse
 ip rip triggered
!
!
router rip
network 192.168.1.0
network 200.1.1.0
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
ip rip split-horizon poisoned-reverse
 ip rip triggered
!
router rip
network 192.168.1.0
network 201.1.1.0
!
```

7. Common Errors

- The triggered updates function is enabled when the RIP configurations at both ends of the link are consistent.
- Both the triggered updates and BFD functions are enabled.
- The triggered updates function is not enabled on all devices on the same link.

1.19.3 Configuring External Routes Imported by RIP

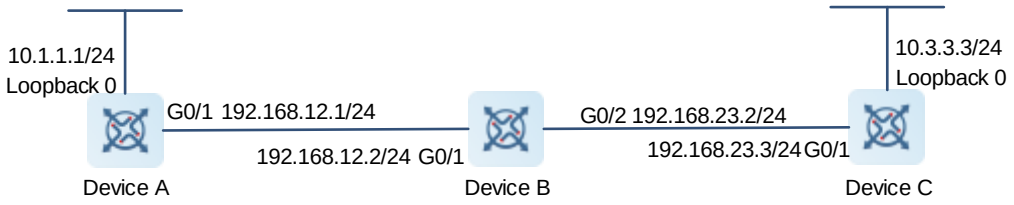
1. Requirements

Device B communicates with Device A through RIP, and Device B obtains the route 10.3.3.3 through a static route.

To enable Device A to obtain the routing information of 10.3.3.3, enable the OSPF routing protocol in Device B. The reliability of introducing external routes is low. Set the external default metric to 5.

2. Topology

Figure 1-11 Topology for Configuring External Routes Imported by RIP



3. Notes

(1) Configure an IP address for each interface and start the unicast routing protocol (omitted).

(2) Configure a static route for Device B.

(3) Configure the basic functions of RIP on Device A and Device B (omitted).

(4) Configure route redistribution on Device B and set the default metric of the redistributed route.

4. Procedure

(1) Configure an IP address for each interface and start the unicast routing protocol (omitted).

(2) Configure a static route to 10.3.3.3/24 on Device B, and set the next hop to 192.168.23.3.

```
Device B> enable
Device B# configure terminal
Device B(config)# ip route 10.3.3.3 255.255.255.0 192.168.23.3
```

(3) Configure the basic functions of RIP on Device A and Device B (omitted).

(4) Set the default metric of the redistributed route to 5 on Device B.

```
Device B(config)# router rip
Device B(config-router)# default-metric 5
```

(5) Configure the redistribution of static route to RIP on Device B.

```
Device B(config-router)# redistribute static
```

5. Verification

Check the routing table on Device A. Verify that the RIP route of 10.3.3.0/24 is available, and the metric is 6.

```
Device A# show ip route rip
R   10.3.3.0/24 [120/6] via 192.168.12.2, 00:06:11, GigabitEthernet 0/1
```

6. Configuration Files

Device B configuration file.

```
!
ip route 10.3.3.3 255.255.255.0 192.168.23.3
!
router rip
 default-metric 5
 redistribute static
!
```

1.19.4 Configuring Increasing the Metric of a RIP Interface

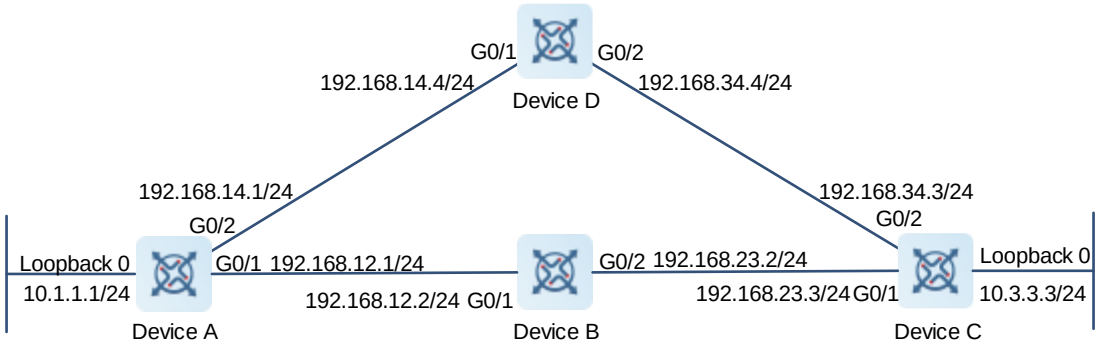
1. Requirements

Device A, Device B, Device C, and Device D implement interworking through the RIPv2 routing protocol.

There are two equal-cost paths from Device A to 10.3.3.3/24 of Device C. In consideration of the old model and low performance of Device D, increase the metric of the Gigabit Ethernet 0/2 interface of Device A so that Device A can go to 10.3.3.3 to prefer Device B.

2. Topology

Figure 1-12 Topology for Increasing the Metric of a RIP Interface



3. Notes

(1) Configure interface IP addresses for all the devices. (Omitted)

(2) Configure the RIP basic functions for all the devices. (Omitted)

(3) Configure ACL on Device C, and enable offset-list on the interface connected to Device B.

4. Procedure

(1) Configure ACL on Device C, and match the route 10.3.3.3/24.

```
Device C> enable
Device C# configure terminal
Device C(config)# access-list 1 permit 10.3.3.3 0.0.0.255
```

(2) Configure **offset** on Device C, associate with ACL 1, and enable the offset-list on the GigabitEthernet 0/2 interface.

```
Device C(config)# router rip
Device C(config-router)# offset-list 1 out 3 gigabitEthernet 0/2
```

5. Verification

Check the routing table of Device A.

```
Device A# show ip route rip
R   10.3.3.0/24 [120/5] via 192.168.14.4, 00:06:11, GigabitEthernet 0/1
```

6. Configuration Files

Device C configuration file.

```
!
access-list 1 permit 10.3.3.3 0.0.0.255
!
```

```
router rip
 offset-list 1 out 3 gigabitEthernet 0/2
!
```

1.19.5 Configuring RIP to Distribute a Summarized Route

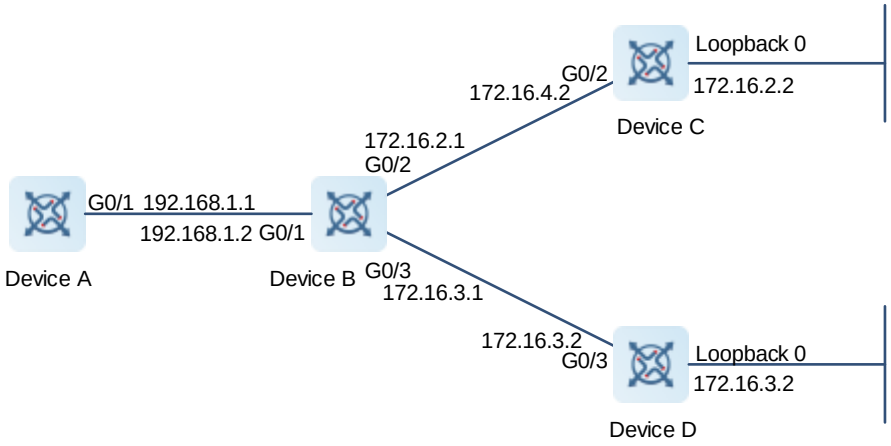
1. Requirements

Device B, implements interworking with Device A, Device C, and Device D through the RIPv2 routing protocol.

To reduce the size of the routing table of Device A, configure route summarization to 172.16.0.0/21 on Device B.

2. Topology

Figure 1-13 Topology for Configuring RIP to Distribute a Summarized Route



3. Notes

(1) Configure interface IP addresses for all devices (omitted).

(2) Configure the RIP basic functions for all the devices (omitted).

(3) Disable automatic summarization on Device B and configure route summarization.

4. Procedure

(1) Configure an IP address for each interface and start the unicast routing protocol (omitted).

(2) Configure RIP basic functions on the devices (omitted).

(3) Disable automatic summarization on Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# router rip
Device B(config-router)# version 2
```

```
Device B(config-router)# no auto-summary
Device B(config-router)# exit
```

(4) Configure 172.16.0.0/21 route summarization on the GigabitEthernet 0/1 interface of Device B.

```
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.248.0
```

5. Verification

Check the routing table of Device A, and verify that the entry 172.16.0.0/16 is generated.

```
Device A# show ip route rip
R 172.16.0.0/21 [120/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1
```

6. Configuration Files

Device B configuration file.

```
!
interface GigabitEthernet 0/1
ip address 196.38.165.1 255.255.255.0
!
router rip
 version 2
 no auto-summary
!
```

Contents

1 Configuring RIPng 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 6
1.2 Configuration Task Summary 6
1.3 Configuring RIPng Basic Functions 7
1.3.1 Overview 7
1.3.2 Restrictions and Guidelines 7
1.3.3 Configuration Tasks 7
1.3.4 Enabling an RIPng Routing Process 7
1.3.5 Configuring RIPng on an Interface 7
1.3.6 Configuring Split Horizon or Poison Reverse 8
1.3.7 Configuring a Passive Interface 9
1.4 Configuring RIPng Route Distribution 9
1.4.1 Overview 9
1.4.2 Configuration Tasks 9
1.4.3 Generating a Default Route 9
1.4.4 Configuring External Route Redistribution 10
1.5 Configuring RIPng Route Filtering Rules 11
1.5.1 Overview 11
1.5.2 Procedure 11

1.6 Configuring to Adjust RIPng Routing 11

1.6.1 Overview 11

1.6.2 Configuration Tasks 11

1.6.3 Configuring to Modify the Management Distance of an RIPng Route 11

1.6.4 Configuring to Modify the Metric Offset on an Interface 12

1.6.5 Configuring the Default Metric of a Route Redistributed to RIPng 12

1.7 Modifying Timers 13

1.7.1 Overview 13

1.7.2 Restrictions and Guidelines 13

1.7.3 Procedure 13

1.8 Enabling GR 14

1.8.1 Overview 14

1.8.2 Restrictions and Guidelines 14

1.8.3 Procedure 14

1.9 Configuring a Super VLAN to Enable RIPng 14

1.9.1 Overview 14

1.9.2 Restrictions and Guidelines 15

1.9.3 Procedure 15

1.10 Monitoring 15

1.11 Configuration Examples 16

1.11.1 Configuring Basic Functions of RIPng 16

1.11.2 Advertising Default Routes/External Routes 19

1 Configuring RIPng

1.1 Introduction

1.1.1 Overview

RIP next generation (RIPng) is a unicast routing protocol that applies to IPv6 networks. RIPng-enabled routers exchange routing information to obtain routes to remote networks.

As an Interior Gateway Protocol (IGP), RIPng can run only within an autonomous system (AS) and is applicable to small-sized networks.

Note

In this chapter, the term “router” refers to any network device that supports the routing function. These network devices can be Layer-3 switches, routers, or firewalls.

1.1.2 Principles

1. Basic Concepts

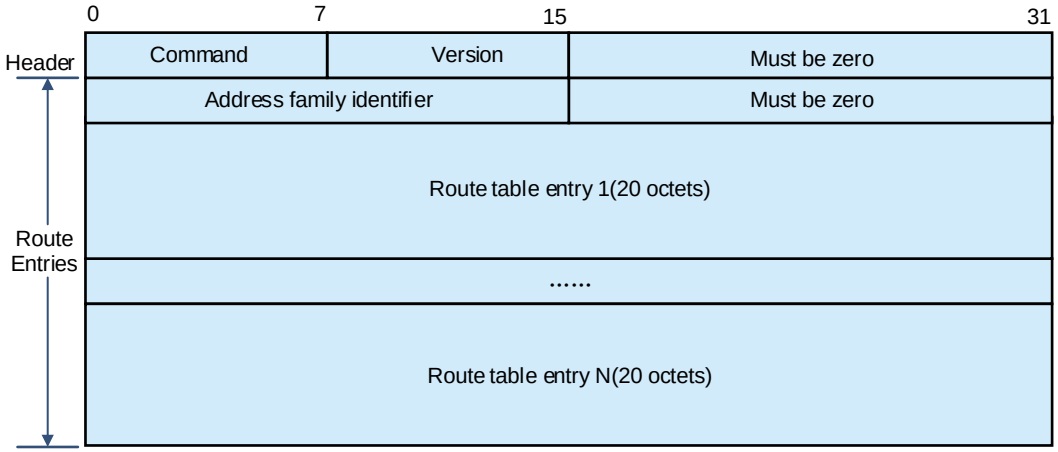
- IGP and EGP

  IGP runs within an AS. For example, RIPng is a type of IGP.

  Exterior Gateway Protocol (EGP) runs between ASs. For example, BGP is a type of EGP.

- RIPng packet format

Figure 1-1 RIPng Packet Format



RIPng packets can contain one or more routing table entries. The number of routing table entries depends on the size of the maximum transmission unit (MTU) value of the interface. Route table entry (RTE) is classified into two types:

- Next hop RTE: Located in the foremost of a set of routing table entries with the same next hop, that is,

the position of Route table entry 1 shown in Figure 1-1.

- IPv6 prefix RTE: Located behind the next hop RTE. Multiple different IPv6 prefix RTEs can exist after a next hop RTE. An IPv6 prefix RTE describes the destination IP address, prefix length, route tag, and metric of an RIPng route.

Figure 1-2 Format of Next Hop RTE

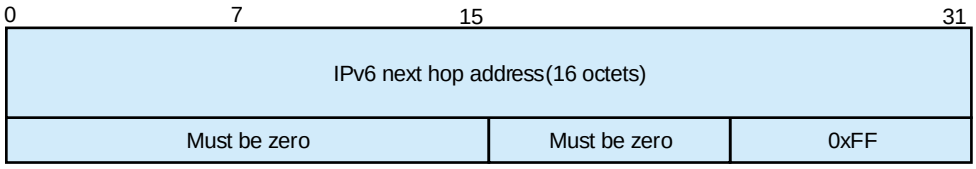
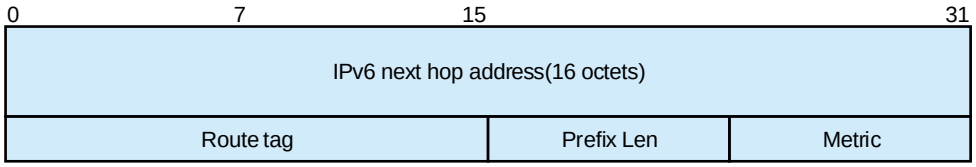


Figure 1-3 Format of IPv6 Prefix RTE



2. RIPng and RIP

RIP applies to IPv4 networks. Two RIP versions are available: RIPv1 and RIPv2.

RIPng is an extension of RIPv2 on the basis of IPv6. Both are similar in functions and configurations. The main differences are as follows:

- The UDP port ID of RIP is 520, and that of RIPng is 521.
- IPv6 features.
  - The RIPv2 multicast address is 224.0.0.9, and the RIPng multicast address is FF02::9.
  - The source address of RIPng route update packets is FE80::/10.

3. Route Control

Compared with static routing, the dynamic routing protocol shows an advantage, that is, by exchanging routing information, devices can automatically obtain routes to a remote network and update the routes in real time.

- Routing switching process

  After RIPng is enabled on a router, the router sends a request packet to its neighbor router, requesting all routing information, that is, the routing table. After receiving the request packet, the neighbor device returns a response packet containing the local routing table. After receiving the response packet, the router updates the local routing table, and sends an update packet to the neighbor router, informing the neighbor router of the route update information. After receiving the update packet, the neighbor router updates the local routing table, and sends the update packet to other adjacent routers. After receiving and processing an update advertisement, all the routers can obtain and retain the latest routing information.
- Periodical update

By default, periodical update is enabled for RIPng. Adjacent routers exchange complete routing information with each other every 30s, that is, the entire routing table is sent to neighbor routers.

Note

For every non-local route, if the route is not updated within 180s (Invalid timer), the metric of the route is changed to 16 (unreachable). If the route is still not updated in the next 120s (Flush timer), the route is deleted from the routing table.

The timer details are as follows:

- Update timer: Route update packets are sent regularly, and the update interval is 30s by default.
- Invalid timer: If an update packet for refreshing the existing route has not been received after 180s (default value), the metric for the route to set to 16, marking the route as invalid.
- Flush timer: By default, the flush timer is set to 240s, 60s greater than the invalid timer. When the flush timer times out, the route is deleted from the routing table.
- Hold-down timer: It prevents route loop caused by route flapping. When the device receives a route update with a cost of 16, the route will be set to hold-down state, and the hold-down timer will be started at the same time. Before the hold-down timer expires, even if an update packet with a metric less than 16 for this route is received, the route will not be updated.

- Default route

  In the routing table, a route to the destination network ::/0 is called default route.

  The default route can be learned from a neighbor device, or sent to a neighbor device.

- Route redistribution

  For RIPng, other types of routes (such as direct routes, static routes, and routes of other routing protocols) are called external routes.

  External routes (excluding the default route) can be redistributed to RIPng and advertised to neighbors.

- Route Filtering

  Filtering conditions can be configured to limit the routing information exchanged between adjacent routers. Only the routing information that meets filtering conditions can be sent or received.

4. Routing Algorithm

RIPng is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.

- Distance-vector algorithm

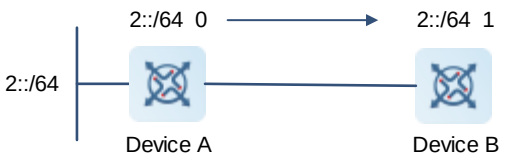
  RIPng is a protocol based on the distance-vector algorithm. The distance-vector algorithm treats a route as a vector that consists of the destination network and distance. The router obtains a route from its neighbor and adds the distance vector from itself to the neighbor to the route to form its own route.

  RIPng uses the hop count to evaluate the distance to the destination network. By default, the hop count from a router to its directly connected network is 0, the hop count from a router to a network that can be reached through a router is 1, and so on. That is, the metric is equal to the number of routers from the local network to the destination network. To restrict the convergence time, RIPng stipulates that the metric must

be an integer in the range from 0 to 15. If the metric is equal to or greater than 16, the destination network or host is unreachable. For this reason, RIPng cannot be applied on a large-scale network.

As shown in Figure 1-4, Device A is connected to the network 2::/64. Device B obtains the route (2::/64, 0) from Device A and adds the metric 1 to the route to obtain its own route (2::/64, 1), and the next hop points to Device A.

Figure 1-4 Diagram of Distance-vector Algorithm

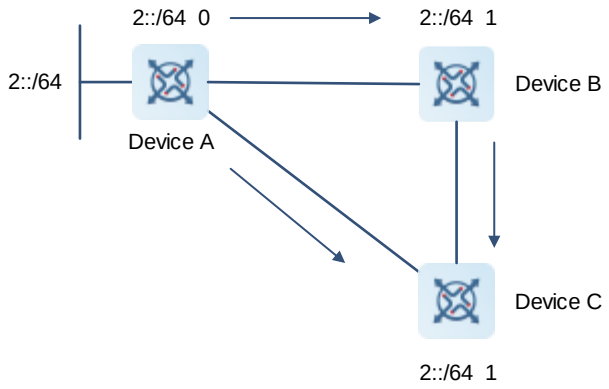


- Selecting the optimum route

  RIPng selects an optimum route based on the following principle: If multiple routes to the same destination network are available, a router preferentially selects the route with the smallest metric.

  As shown in Figure 1-5, Device A is connected to the network 2::/64. Device C obtains the route (2::/64, 0) from Device A and the route (2::/64, 1) from Device B. Device C will select the route that is obtained from Device A and add metric 1 to this route to form its own route (2::/64, 1), and the next hop points to Device A.

Figure 1-5 Diagram of Selecting the Optimum Route



Note

When routes coming from different sources exist on a router, the route with the smallest distance is preferentially selected.

Table 1-1 Distance-vector Table

Route Source	Default Distance
Directly-connected network	0
Static route	1

Route Source	Default Distance
OSPF route	110
IS-IS route	115
RIP route	120
Unreachable route	255

5. Avoiding Route Loops

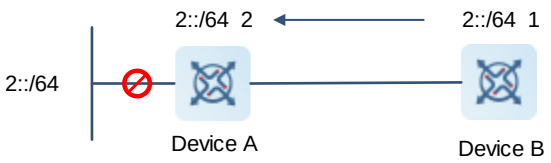
RIPng uses functions such as split horizon and poison reverse to avoid route loops.

- Route loop

  An RIPng route loop occurs due to inherent defects of the distance-vector algorithm.

  As shown in Figure 1-6, Device A is connected to the network 2::/ 64, and sends an update packet every 30s. Device B receives the route to 2::/64 from Device A every 30s. If Device A is disconnected from 2::/64, the route to 2::/64 will be deleted from the routing table on Device A. Next time, the update packet sent by Device A no longer contains this route. As Device B does not receive an update packet related to 2::/64, Device B determines that the route to 2::/64 is valid within 180s and uses the update packet to send this route to Device A. As the route to 2::/64 does not exist on Device A, the route learned from Device B is added to the routing table. Device B determines that data can reach 2::/64 through Device A, and Device A determines that data can reach 2::/64 through Device B. In this way, a route loop is formed.

Figure 1-6 Diagram of Route Loop

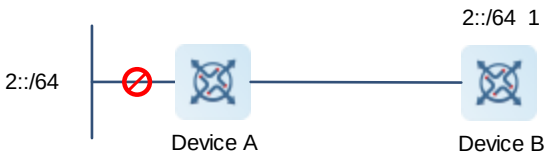


- Split horizon

  Split horizon can prevent route loops. After split horizon is enabled, a route received on this interface will not be sent out from this interface.

  As shown in Figure 1-7, after split horizon is enabled on Device B, Device B will not send the route to 2::/64 back to Device A. Device B will learn 180s later that 2::/64 is not reachable.

Figure 1-7 Diagram of Split Horizon



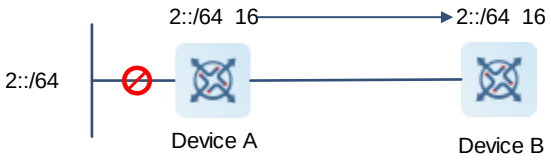
- Poison reverse

Poison reverse can also prevent route loops. Compared with slit horizon, poison reverse is more reliable, but brings more protocol packets, which makes network congestion more severe.

After poison reverse is enabled on an interface, a route received from this interface will be sent out from this interface again, but the metric of this router will be changed to 16 (unreachable).

As shown in Figure 1-8, after poison reverse is enabled on Device A, if Device A detects a disconnection from 2::/64, Device A will not delete the route to 2::/64. Instead, Device A changes the number of hops to **16**, and advertises the route through the update packet. Upon receiving the update packet, Device B learns that 2::/64 is not reachable.

Figure 1-8 Diagram of Poison Reverse



1.1.3 Protocols and Standards

- RFC2080: RIPng for IPv6
- RFC 2081: RIPng Protocol Applicability Statement

1.2 Configuration Task Summary

The RIPng configuration includes the following tasks:

(1) Configuring RIPng Basic Functions

a Enabling an RIPng Routing Process

b Configuring RIPng on an Interface

c (Optional) Configuring Split Horizon or Poison Reverse

d (Optional) Configuring a Passive Interface

(2) (Optional) Configuring RIPng Route Distribution The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Generating a Default Route
- Configuring External Route Redistribution

(3) (Optional) Configuring RIPng Route Filtering Rules

(4) (Optional) Configuring to Adjust RIPng Routing The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Modify the Management Distance of an RIPng Route
- Configuring to Modify the Metric Offset on an Interface
- Configuring the Default Metric of a Route Redistributed to RIPng Metric

(5) (Optional) Modifying Timers

(6) (Optional) Enabling GR

(7) (Optional) Configuring a Super VLAN to Enable RIPng

1.3 Configuring RIPng Basic Functions

1.3.1 Overview

This function can be used to build an RIPng routing domain on the network, and routers in the domain obtain routes to a remote network through RIPng.

1.3.2 Restrictions and Guidelines

- IPv6 addresses must be configured.
- IPv6 unicast routes must be enabled.

1.3.3 Configuration Tasks

The basic function configuration of RIPng includes the following tasks:

(1) Enabling an RIPng Routing Process

(2) Configuring RIPng on an Interface

(3) (Optional) Configuring Split Horizon or Poison Reverse

(4) (Optional) Configuring a Passive Interface

1.3.4 Enabling an RIPng Routing Process

1. Overview

This command is used to create an RIPng routing process and enter routing process configuration mode.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable an RIPng routing process and enter route configuration mode.

ipv6 router rip

The RIPng routing process is disabled by default.

1.3.5 Configuring RIPng on an Interface

1. Overview

In RIPv2, the **network** command is configured in routing process configuration mode to define an IP address range. In RIPng, if the IP address of an interface belongs to this IP address range, RIPng automatically runs on this interface.

After RIPng runs on an interface, RIPng packets can be exchanged on the interface and RIPng can learn routes to the network segments directly connected to the device.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure RIPng on an interface.

ipv6 rip enable

By default, an interface is not added to the RIPng process.

1.3.6 Configuring Split Horizon or Poison Reverse

1. Overview

Split horizon can prevent route loops. After split horizon is enabled, a route received on this interface will not be sent out from this interface.

After poison reverse is enabled on an interface, a route received from this interface will be sent out from this interface again, but the metric will be changed to **16** (unreachable).

2. Restrictions and Guidelines

- You are advised to enable split horizon on the interfaces of broadcast type network (such as Ethernet) and point-to-point type network (such as PPP and HDLC). (Retain the default setting.)
- It is recommended that split horizon and poison reverse be disabled on an interface to a non-broadcast multi-access network such as FR and X.25; otherwise, some devices cannot learn the complete routing information.
- If the secondary IP address is configured for an interface connected to a non-broadcast network, it is recommended that split horizon and poison reverse be disabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Configure split horizon.

split-horizon [**poisoned-reverse**]

By default, split horizon is enabled and poison reverse is disabled on an interface.

1.3.7 Configuring a Passive Interface

1. Overview

A passive interface is set with the boundary of RIPng routing domain. The network segment of the passive interface belongs to the RIPng routing domain, but RIPng packets cannot be sent over the passive interface.

The interface set to a passive interface suppresses RIPng update packets. The passive interface defines the boundary of RIPng routing domain to avoid unwanted flooding of RIPng packets. If the interface connection device does not run the RIPng routing protocol (such as a PC and a device running other routing protocols), you are advised to configure this interface as a passive interface.

2. Restrictions and Guidelines

If RIPng routes need to be exchanged on an interface (such as the router interconnect interface) in the RIPng routing domain, this interface cannot be configured as a passive interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Configure passive interfaces.

passive-interface { **default** | *interface-type interface-number* }

The passive interface function is disabled by default.

1.4 Configuring RIPng Route Distribution

1.4.1 Overview

RIPng can distribute the routes of other routing protocols or default routes in the local routing domain so that the devices in the routing domain can access other routing domains.

1.4.2 Configuration Tasks

The configuration of RIPng route distribution includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Generating a Default Route
- Configuring External Route Redistribution

1.4.3 Generating a Default Route

1. Overview

This function is used to introduce a default route to an AS edge router so that other routers in the RIPng domain access other AS domains through this AS edge router by default. In the routing table, a route to the destination network ::/0 is called default route. The default route can be learned from a neighbor device, or sent to a

neighbor device. Please configure and distribute the default route according to the actual situation of networking, or specify the cost of the distributed default route.

2. Restrictions and Guidelines

- When there are no special requirements and this command is configured on the interface, an IPv6 default route is advertised to the external devices through this interface, but the route itself is not added to the route forwarding table of the device and the RIPng route database.
- To prevent occurrence of a route loop, once this command is configured on an interface, RIPng refuses to receive the default route updates advertised by neighbors.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure external route redistribution.

ipv6 rip default-information { **only** | **originate** } [**metric** *metric-value*]

1.4.4 Configuring External Route Redistribution

1. Overview

This function is used to introduce external routes of the RIPng domain to the AS edge device.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Generate a default route.

redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [**metric** *metric-value* | **route-map** *route-map-name*] *

The redistribution function is not configured by default. This function redistributes the routes of all subtypes of the specified routing process.

1.5 Configuring RIPng Route Filtering Rules

1.5.1 Overview

Routes that do not meet filtering criteria cannot be loaded to the routing table, or advertised to neighbors. In this way, users within the network can be prevented from accessing specified destination networks.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a prefix list.

ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

(4) Enter the routing process configuration mode.

ipv6 router rip

(5) Configure to filter the received RIP routing information.

distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-number*]

By default, the distribution list is disabled.

1.6 Configuring to Adjust RIPng Routing

1.6.1 Overview

Change the RIPng routes to enable the traffic pass through specified nodes or avoid passing through specified nodes. Change the sequence that a router selects various types of routes so as to change the priorities of RIPng routes.

1.6.2 Configuration Tasks

The configuration for modifying routing parameters includes the following tasks, and these tasks are optional. Select tasks for configuration according to actual condition.

- Configuring to Modify the Management Distance of an RIPng Route
- Configuring to Modify the Metric Offset on an Interface
- Configuring the Default Metric of a Route Redistributed to RIPng Metric

1.6.3 Configuring to Modify the Management Distance of an RIPng Route

1. Overview

This function is used to set the management distance of an RIPng route and change the priority of a router in routing.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Configure to modify the management distance of an RIPng route.

distance *distance*

The management distance is **120** by default.

1.6.4 Configuring to Modify the Metric Offset on an Interface

1. Overview

Before a route is added to the routing table, the metric of the route must be added with the metric offset set on the interface. You can control the use of a route by setting the interface metric offset.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to modify the metric offset to be added to the interface of an RIPng route.

ipv6 rip metric-offset *value*

By default, the metric on an interface is **1**.

1.6.5 Configuring the Default Metric of a Route Redistributed to RIPng

1. Overview

The default metric of a redistributed route is **1**. If you want to preferably select an internal RIP route on some networks, just increase the default metric.

2. Restrictions and Guidelines

- Unless otherwise required, perform this configuration on an AS edge device to which external routes are introduced.
- If the metric is not specified during redistribution of a routing protocol process, RIPng uses the metric defined by the **default-metric** command. If the metric is specified, the metric defined by the **default-metric** command is overwritten by the specified metric.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Configure the default metric of a route redistributed to RIPng.

default-metric *metric*

By default, the metric for route redistribution is 1.

1.7 Modifying Timers

1.7.1 Overview

By adjusting the timers, you can reduce the convergence time and fault rectification time of the routing protocol. For devices connected to the same network, values of the three RIPng timers must be the same. Generally, you are not advised to modify the RIP timers unless otherwise required.

Setting timers to small values on a low-speed link brings risks because a lot of Update packets consume the bandwidth. You can set timers to small values generally on the Ethernet or a 2 Mbps (or above) link to reduce the convergence time of network routes.

1.7.2 Restrictions and Guidelines

- The RIPng basic functions must be configured.
- Modifying the protocol control parameters may result in protocol running failures. Therefore, you are advised not to modify the timers.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Configure to modify the RIPng timers.

timers *update invalid flush*

By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

1.8 Enabling GR

1.8.1 Overview

GR ensures uninterrupted data transmission when the protocol is restarted. The GR period is the maximum time from restart of the RIPng process to completion of GR. During this period, the forwarding table before the restart is retained, and the RIPng route is restored so as to restore the RIPng state before the restart. After the restart period expires, RIPng exits the GR state and performs common RIPng operations.

1.8.2 Restrictions and Guidelines

- The RIPng basic functions must be configured.
- The GR period is at least twice the RIP route update period.
- The **graceful-restart grace-period** command allows you to explicitly modify the GR period. Note that GR must be completed before the invalid timer of the RIPng route expires. An inappropriate GR period cannot ensure uninterrupted data forwarding during the GR process. A typical case is as follows: If the GR period is longer than the duration of the invalid timer, GR is not completed when the invalid timer expires. The route is not re-advertised to the neighbor, and forwarding of the route of the neighbor stops after the invalid timer expires, causing interruption of data forwarding on the network. Unless otherwise required, you are not advised to adjust the GR period. If it is necessary to adjust the GR period, ensure that the GR period is at least twice the RIP route update period based on the configuration of the **timers** command. The GR period must be also smaller than the duration of the invalid timer.
- During the RIPng GR process, ensure that the network environment is stable.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the routing process configuration mode.

ipv6 router rip

(4) Enable GR.

graceful-restart [**grace-period** *grace-period*]

The GR function is enabled by default.

1.9 Configuring a Super VLAN to Enable RIPng

1.9.1 Overview

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when RIP multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIP multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing protocol flapping.

In most scenarios, the RIPng function does not need to be enabled on a super VLAN, and it is disabled by default. However, in some scenarios, the RIPng function must be run on the super VLAN, but packets need to be sent to only one sub VLAN. In this case, you can decide to send multicast packets to a certain sub VLAN or to all sub VLANs as actually needed. You can run this command to specify a particular sub VLAN. You must be cautious when configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

1.9.2 Restrictions and Guidelines

- The RIPng basic functions must be configured.
- The designated sub VLAN must be connected to neighbors.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the SVI interface mode.

interface vlan *vlan-id*

(4) Configure a super VLAN to enable RIPng.

ipv6 rip subvlan [**all** | *vlan-id*]

By default, the RIPng function is disabled on a super VLAN.

1.10 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2

Command	Purpose
show ipv6 rip	Displays information about the RIPng process.
show ipv6 rip database	Displays the RIPng routing table.
debug ipv6 rip [interface *interface-type interface-number* | **nsm** | **restart** | **event** [**ipsec**]]	Debugs RIPng.

1.11 Configuration Examples

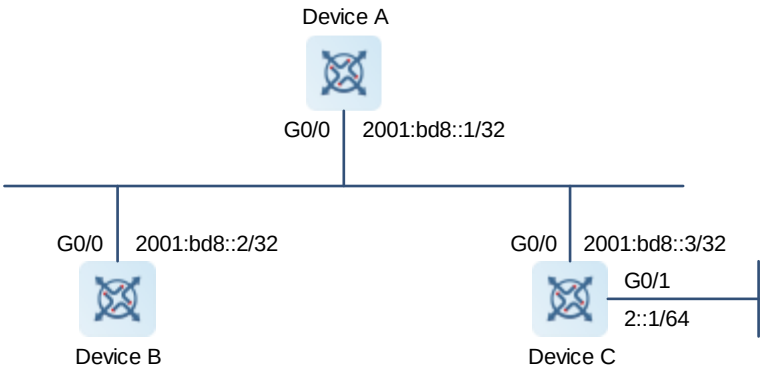
1.11.1 Configuring Basic Functions of RIPng

1. Requirements

On an IPv6 network, configure RIPng to realize internetworking.

2. Topology

Figure 1-9 Topology for Basic Features of RIPng



3. Notes

- Configure IPv6 addresses on the related devices.
- Enable the RIPng routing function on all the devices.

4. Procedure

(1) Configure an IPv6 address for each interface.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/0
Device A(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::1/32
Device A(config-if-GigabitEthernet 0/0)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/0
Device B(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::2/32
Device B(config-if-GigabitEthernet 0/0)# exit
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface GigabitEthernet 0/0
```

```
Device C(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::3/32
Device C(config-if-GigabitEthernet 0/0)# exit
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ipv6 address 2::1/64
Device C(config-if-GigabitEthernet 0/1)# exit
```

(2) Enable the RIPng routing function on all the devices.

Configure Device A.

```
Device A(config)# ipv6 router rip
Device A(config-router)# exit
Device A(config)# interface GigabitEthernet 0/0
Device A(config-if-GigabitEthernet 0/0)# ipv6 rip enable
```

Configure Device B.

```
Device B(config)# ipv6 router rip
Device B(config-router)# exit
Device B(config)# interface GigabitEthernet 0/0
Device B(config-if-GigabitEthernet 0/0)# ipv6 rip enable
```

Configure Device C.

```
Device C(config)# ipv6 router rip
Device C(config-router)# exit
Device C(config)# interface GigabitEthernet 0/0
Device C(config-if-GigabitEthernet 0/0)# ipv6 rip enable
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ipv6 rip enable
```

5. Verification

Check the routing tables of Device A, Device B, and Device C. Verify that RIPng has learned the routes to remote networks.

- Check the routing table of Device A.

```
Device A# show ipv6 route
IPv6 routing table name - Default - 6 entries
Codes:  C - Connected, L - Local, S - Static
   R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
   E1 - OSPF external type 1, E2 - OSPF external type 2
   SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
   IA - Inter area

R     2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0
C     2001:DB8::/32 via GigabitEthernet 0/0, directly connected
L     2001:DB8::1/128 via GigabitEthernet 0/0, local host
C     FE80::/10 via ::1, Null0
C     FE80::/64 via GigabitEthernet 0/0, directly connected
L     FE80::2D0:F8FF:FEFB:E7CE/128 via GigabitEthernet 0/0, local host
```

- Check the routing table of Device B.

```
Device B# show ipv6 route

IPv6 routing table name - Default - 6 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

R     2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0
C     2001:DB8::/32 via GigabitEthernet 0/0, directly connected
L     2001:DB8::2/128 via GigabitEthernet 0/0, local host
C     FE80::/64 via GigabitEthernet 0/0, directly connected
L     FE80::2D0:F8FF:FEFB:C9BA/128 via GigabitEthernet 0/0, local host
```

- Check the routing table of Device C.

```
Device C# show ipv6 route

IPv6 routing table name - Default - 9 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

C     2::/64 via GigabitEthernet 0/1, directly connected
L     2::2/128 via GigabitEthernet 0/1, local host
C     2001:DB8::/32 via GigabitEthernet 0/0, directly connected
L     2001:DB8::3/128 via GigabitEthernet 0/0, local host
C     FE80::/10 via ::1, Null0
C     FE80::/64 via GigabitEthernet 0/0, directly connected
L     FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/0, local host
C     FE80::/64 via GigabitEthernet 0/1, directly connected
L     FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/1, local host
```

6. Configuration Files

- Device A configuration file

```
!
ipv6 router rip
!
interface GigabitEthernet 0/0
 ipv6 address 2001:db8::1/32
 ipv6 rip enable
!
```

- Device B configuration file

```
!
ipv6 router rip
!
interface GigabitEthernet 0/0
 ipv6 address 2001:db8::2/32
 ipv6 rip enable
!
```

- Device C configuration file

```
!
ipv6 router rip
!
interface GigabitEthernet 0/0
 ipv6 address 2001:db8::3/32
 ipv6 rip enable
!
interface GigabitEthernet 0/1
 ipv6 address 2::1/64
 ipv6 rip enable
!
```

7. Common Errors

- The IPv6 address is not configured on an interface.
- The interface used for interworking between devices is configured as a passive interface.

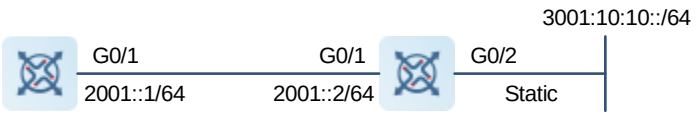
1.11.2 Advertising Default Routes/External Routes

1. Requirements

On a network adopting OSPFv3 networking, Device A and Device B are egress devices on the network, Device A is the default egress used to advertise the default route to Device B, and Device B communicates with the internal network through a static route.

2. Topology

Figure 1-10 Topology for Advertising Default Routes/External Routes



3. Notes

- Configure interface IPv6 addresses for all devices (omitted).
- Configure the RIPng basic functions on all devices (omitted).
- Redistribute the static route on Device B.
- On the GigabitEthernet 0/1 interface of Device A, configure advertisement of the default route.

4. Procedure

(1) Configure redistribution of a static route on Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# ipv6 router rip
Device B(config-router)# redistribute static
```

(2) Configure redistribution of a default route on Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 rip default-information originate
```

5. Verification

Check the routing tables on Device A and Device B, and verify that Device A can learn the route 3001:10:10::/64, and Device B can learn the default route ::/0.

```
Device A# show ipv6 route rip

IPv6 routing table name - Default - 17 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area
R     3001:10:10::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1
Device B# show ipv6 route rip

IPv6 routing table name - Default - 17 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area
R     ::/0 [120/2] via FE80::21A:A9FF:FE41:5B06, GigabitEthernet 0/1
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 ipv6 rip default-information originate
!
```

- Device B configuration file

```
!
```

```
ipv6 router rip
 redistribute static
!
```

Contents

1 Configuring OSPF v2 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 2
1.1.3 Protocols and Standards 25
1.2 Configuration Task Summary 26
1.3 Configuring Basic Features 28
1.3.1 Overview 28
1.3.2 Restrictions and Guidelines 28
1.3.3 Configuration Tasks 29
1.3.4 Configuring OSPF Process 29
1.3.5 Configuring Router ID 29
1.3.6 Adding Interface IP to OSPF and Specifying Area ID 30
1.3.7 Enabling OSPF on an Interface and Specifying an Area ID 31
1.3.8 Creating a Virtual Link 31
1.4 Configuring OSPF Network Type 32
1.4.1 Overview 32
1.4.2 Restrictions and Guidelines 32
1.4.3 Configuration Tasks 33
1.4.4 Configuring the Interface Network Type 33
1.4.5 Configuring a Neighbor 34

1.4.6 Configuring the Interface Priority 35

1.4.7 Disabling Source Address Verification 35

1.5 Adjusting OSPF Routing 36

1.5.1 Overview 36

1.5.2 Restrictions and Guidelines 36

1.5.3 Configuration Tasks 36

1.5.4 Configuring the AD 37

1.5.5 Configuring the Reference Bandwidth 37

1.5.6 Configuring the Cost of an Interface 38

1.5.7 Configuring Cost Fallback Value for an AP 39

1.5.8 Configuring the Cost of the Default Route in a Stub Area or an NSSA 39

1.5.9 Configuring the Default Metric Value for Redistribution 40

1.5.10 Configuring the Maximum Metric 41

1.5.11 Configuring RFC1583 Compatibility 42

1.5.12 Configuring Association of External Route Forwarding Addresses with Interface Configuration 42

1.6 Configuring OSPF Route Advertisement 43

1.6.1 Overview 43

1.6.2 Restrictions and Guidelines 44

1.6.3 Configuration Tasks 44

1.6.4 Configuring External Route Redistribution 44

1.6.5 Generating a Default Route 45

1.6.6 Configuring a Device as ASBR 46

1.7 Configuring OSPF Route Summarization 47
1.7.1 Overview 47
1.7.2 Restrictions and Guidelines 47
1.7.3 Configuration Tasks 47
1.7.4 Configuring Inter-Area Route Summarization 47
1.7.5 Configuring External Route Summarization 48
1.7.6 Configuring a Discard Route 49
1.8 Configuring OSPF Route Filtering 49
1.8.1 Overview 49
1.8.2 Restrictions and Guidelines 50
1.8.3 Configuration Tasks 50
1.8.4 Configuring a Passive Interface 50
1.8.5 Configuring LSA Update Packet Filtering 50
1.8.6 Configuring Inter-area Route Filtering 51
1.8.7 Configuring Redistributed Route Filtering 52
1.8.8 Configuring Learned Route Filtering 53
1.9 Adjusting OSPF Network Convergence Speed 54
1.9.1 Overview 54
1.9.2 Restrictions and Guidelines 54
1.9.3 Configuration Tasks 54
1.9.4 Configuring the Hello Interval 54
1.9.5 Configuring the Dead Interval 55
1.9.6 Configuring LSU Transmission Delay 56

1.9.7 Configuring LSU Retransmission Interval....57

1.9.8 Configuring LSU Generation Time....57

1.9.9 Configuring LSA Group Refresh Time....58

1.9.10 Configuring LSA Group Refresh Interval....59

1.9.11 Configuring Duplicate LSA Receiving Delay....59

1.9.12 Configuring Inter-Area Route Computation Delay....60

1.9.13 Configuring External Route Computation Delay....60

1.9.14 Configuring SPF Computation Delay....61

1.9.15 Enabling Two-Way Maintenance....62

1.10 Configuring Stub Area and NSSA....62

1.10.1 Overview....62

1.10.2 Restrictions and Guidelines....62

1.10.3 Configuration Tasks....63

1.10.4 Configuring a Stub Area....63

1.10.5 Configuring an NSSA....64

1.11 Configuring OSPF Authentication....65

1.11.1 Overview....65

1.11.2 Restrictions and Guidelines....65

1.11.3 Configuration Tasks....65

1.11.4 Configuring the Authentication Type of an Area....65

1.11.5 Configuring the Authentication Type of an Interface....66

1.11.6 Configuring a Plain Text Authentication Key for an Interface....67

1.11.7 Configuring an MD5 Authentication Key for an Interface....68

1.12 Enabling Fast Reroute 68
1.12.1 Overview 68
1.12.2 Restrictions and Guidelines 69
1.12.3 Configuration Tasks 69
1.12.4 Configuring Fast Reroute 69
1.12.5 Configuring Interface LFA Protection 70
1.12.6 Preventing an Interface From Becoming a Backup Interface 70
1.13 Modifying the Maximum Number of Concurrent Neighbors 71
1.13.1 Overview 71
1.13.2 Restrictions and Guidelines 71
1.13.3 Configuration Tasks 71
1.13.4 Configuring the Maximum Number of Concurrent Neighbors on the Current Process 71
1.13.5 Configuring the Maximum Number of Concurrent Neighbors on All Processes 72
1.14 Configuring the GR Function 72
1.14.1 Overview 72
1.14.2 Restrictions and Guidelines 73
1.14.3 Configuration Tasks 73
1.14.4 Enabling the GR Function 73
1.14.5 Configuring the OSPF GR Helper Function 74
1.15 Correlating OSPF with BFD 75
1.15.1 Overview 75
1.15.2 Restrictions and Guidelines 75
1.15.3 Configuration Tasks 75

1.15.4 Configuring BFD Correlation with OSPF on an Interface 75

1.15.5 Configuring BFD Correlation with OSPF Globally 76

1.16 Enabling Overflow 76

1.16.1 Overview 76

1.16.2 Restrictions and Guidelines 77

1.16.3 Configuration Tasks 77

1.16.4 Configuring the Memory Overflow Function 77

1.16.5 Configuring the Database Overflow Function 78

1.16.6 Configuring the External LSA Database Overflow Function 78

1.17 Configuring VPN Extended Feature of OSPF 79

1.17.1 Overview 79

1.17.2 Restrictions and Guidelines 79

1.17.3 Configuration Tasks 79

1.17.4 Configuring Domain ID 80

1.17.5 Configuring a Domain Label 80

1.17.6 Configuring a Sham Link 81

1.17.7 Disabling Loop Detection for a VRF OSPF Process 82

1.17.8 Configuring Extcommunity Attribute for a VPN Route 83

1.17.9 Disabling Loop Detection Using the DN Bit of LSA 84

1.17.10 Disabling Loop Detection Using the Route Tag of LSA 85

1.18 Configuring Network Management Functions 85

1.18.1 Overview 85

1.18.2 Restrictions and Guidelines 85

1.18.3 Configuration Tasks 86

1.18.4 Binding the MIB with an OSPF Process 86

1.18.5 Configuring the Trap Function 86

1.18.6 Configuring the Logging Function 87

1.19 Enabling NSR 88

1.19.1 Overview 88

1.19.2 Restrictions and Guidelines 88

1.19.3 Procedure 88

1.20 Enabling the iSPF Feature 89

1.20.1 Overview 89

1.20.2 Restrictions and Guidelines 89

1.20.3 Procedure 89

1.21 Configuring to Disable MTU Verification 89

1.21.1 Overview 89

1.21.2 Restrictions and Guidelines 89

1.21.3 Procedure 90

1.22 Configuring a Super VLAN to Enable OSPF 90

1.22.1 Overview 90

1.22.2 Restrictions and Guidelines 90

1.22.3 Procedure 90

1.23 Monitoring 91

1.24 Configuration Examples 93

1.24.1 Configuring Basic Functions of OSPF 93

1.24.2 Configuring a Stub Area.....97

1.24.3 Configuring an NSSA.....99

1.24.4 Correlating OSPF Process with BFD.....102

1.24.5 Configuring Fast Reroute.....105

1.24.6 Configuring Network Management Functions 106

1.24.7 Configuring the Sham Link Function 109

1.24.8 Configuring a Virtual Link.....120

1.24.9 Selecting a DR of OSPF 122

1 Configuring OSPF v2

1.1 Introduction

1.1.1 Overview

The open shortest path first (OSPF) is an Interior Gateway Protocol (IGP) that is used within the autonomous system (AS) to allow routers to obtain a route to a remote network.

In the early stage after dynamic routing emerges, Routing Information Protocol (RIP) was mainly used on the network. RIP is a distance vector routing protocol, facing some problems such as slow convergence, routing loop, poor scalability, and use for simple networks only. OSPF Version 2 (OSPFv2) is a link state routing protocol, which can effectively fix the above problems. Therefore, OSPFv2 is widely used on large and medium-sized networks.

Note

- OSPFv2 is applicable to IPv4, and OSPF Version 3 (OSPFv3) is applicable to IPv6. The protocol running mechanism and most configurations are the same.
- Unless otherwise specified, "OSPF" in the following descriptions refers to OSPFv2.

OSPF has the following characteristics:

- Wide scope of application: OSPF is applicable to a larger-scale network that supports hundreds of routers.
- Fast convergence: Once the network topology changes, advertisements can be quickly sent between routers to update routes.
- No self-loop: Only the link status information is synchronized between routers. Each router computes routes independently, and a self-loop will not occur.
- Area division: A large routing domain is divided into multiple small areas to save system resources and network bandwidth and ensure stability and reliability of routes.
- Route classification: Routes are classified into several types to support flexible control.
- Equivalent routes: OSPF supports equivalent routes.
- Authentication: OSPF supports packet authentication to ensure security of protocol interaction.
- Multicast transmission: Protocol packets are sent using the multicast address to avoid interfering with irrelevant entities and save system resources.

Note

In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be Layer-3 switches, routers, or firewalls.

1.1.2 Principles

1. Simple Principles

OSPF is a type of link-state routing protocols. Its working process consists of three phases:

(1) Neighbor discovery → Bidirectional communication: An OSPF neighbor relationship is set up between adjacent routers, and bidirectional communication is maintained.

(2) Database synchronization → Full adjacency: A router uses link-state advertisements (LSAs) to advertise all its link states. LSAs are exchanged between neighbors and the link state database (LSDB) is synchronized to achieve full adjacency.

(3) Shortest path tree (SPT) computation → Formation of a routing table: The router computes the shortest path to each destination network based on the LSDB and forms an OSPF routing table.

- Neighbor discovery → Bidirectional communication

  Routers send hello packets through all OSPF-enabled interfaces or virtual links. If hello packets can be exchanged between two routers, and parameters carried in the hello packets can be successfully negotiated, the two routers become neighbors. Routers that are mutual neighbors find their own router IDs from hello packets sent from neighbors, and bidirectional communication is set up.

  A hello packet includes, but is not limited to, the following information:

  - Router ID of the originating router.
  - Area ID of the originating router interface or virtual link.
  - Subnet mask of the originating router interface or virtual link.
  - Authentication information of the originating router interface or virtual link.
  - Hello interval of the originating router interface or virtual link.
  - Neighbor dead interval of the originating router interface or virtual link.
  - IP addresses of the designated router (DR) and backup designated router (BDR).
  - Priority of the originating router interface (used for DR/BDR election).
  - Router ID of the neighbor of the originating router.

- Database synchronization → Full adjacency

  After bidirectional communication is established between neighbor routers, database description (DD), link state request (LSR), link state update (LSU), and link state acknowledgment (LSAck) packets are used to exchange LSAs and establish an adjacency relationship. The brief process is as follows:

  - A router generates an LSA to describe all link states on the router.
  - The LSA is exchanged between neighbors. When a router receives the LSA from its neighbor, it copies the LSA and saves the copy in the local LSDB, and then advertises the LSA to other neighbors.
  - When the router and its neighbors obtain the same LSDB, full adjacency is achieved.

Note

OSPF will not generate LSDB updates and advertisements without changes in link costs or network addition/deletion. If any change takes place, the changed link states are advertised to quickly synchronize the LSDB.

- SPT computation → Formation of a routing table

  After the complete LSDB is obtained from the router, the Dijkstra algorithm is run to generate an SPT from the local router to each destination network. The SPT records the destination networks, next-hop addresses, and costs. OSPF generates a routing table based on the SPT.

  If changes in link costs or network addition/deletion take place, the LSDB will be updated. The router again runs the Dijkstra algorithm, generates a new SPT, and updates the routing table.

Note

The Dijkstra algorithm is used to find the shortest path from a vertex to other vertices in a weighted directed graph.

2. Basic Concepts

- Routing domain

  All routers in an AS must be interconnected and use the same routing protocol. Therefore, an AS is also called a routing domain.

  An AS on which OSPF runs is also called OSPF routing domain, or OSPF domain for short.

- OSPF process

  OSPF supports multiple instances, and each instance corresponds to an OSPF process. One or more OSPF processes can be started on a router. Each OSPF process runs OSPF independently, and the processes are mutually isolated. The process ID takes effect only on the local router, and does not affect exchange of OSPF packets on adjacent interfaces.

- Router ID

  The router ID uniquely identifies a router in an OSPF domain. Router IDs of any two routers cannot be the same.

  If multiple OSPF processes exist on a router, each OSPF process uses one router ID. Router IDs of any two OSPF processes cannot be the same.

  A router ID can be manually configured or automatically selected by the router. You are advised to select manual configuration. If no router ID is specified manually, the automatic selection rules are as follows:

  a The largest IP address from the lookback interface addresses is selected as the router ID;

  b If no lookback interface is configured, the largest IP address from the physical interface addresses is selected as the router ID.

- Area

OSPF supports multiple areas. An OSPF domain is divided into multiple areas to ease the computing pressure of a large-scale network.

An area is a logical group of routers, and each group is identified by an area ID. The border between areas is a router. A router may belong to one area or multiple areas. One network segment (link) can belong to only one area, or each OSPF-enabled interface must belong to a specified area.

- Backbone area and normal area

  Area 0 is the backbone area, and other areas are normal areas. Normal areas must be directly connected to the backbone area.

- Stub area (OSPF stubby area)

  Configuring a stub area can reduce the number of LSAs in the area. The area border router (ABR) in the stub area will not transfer the Type-5 LSA (external route), and will advertise the default route to the stub area.

- Totally stub area

  A totally stub area is upgraded from a stub area. The router in the totally stub area will not transfer Type-3 LSA (inter-domain route) and Type-5 LSA (external route), and will advertise the default route to the stub area.

- Not-so-stubby area (NSSA)

  An NSSA is similar to a stub area, but allows the autonomous system boundary router (ASBR). The route redistributed by ASBR will be transferred in the NSSA area in the form of Type-7 LSA, and the Type-7 LSA will be converted into Type-5 LSA on ABR and then transferred to other areas. The ABR also advertises the default route to the NSSA.

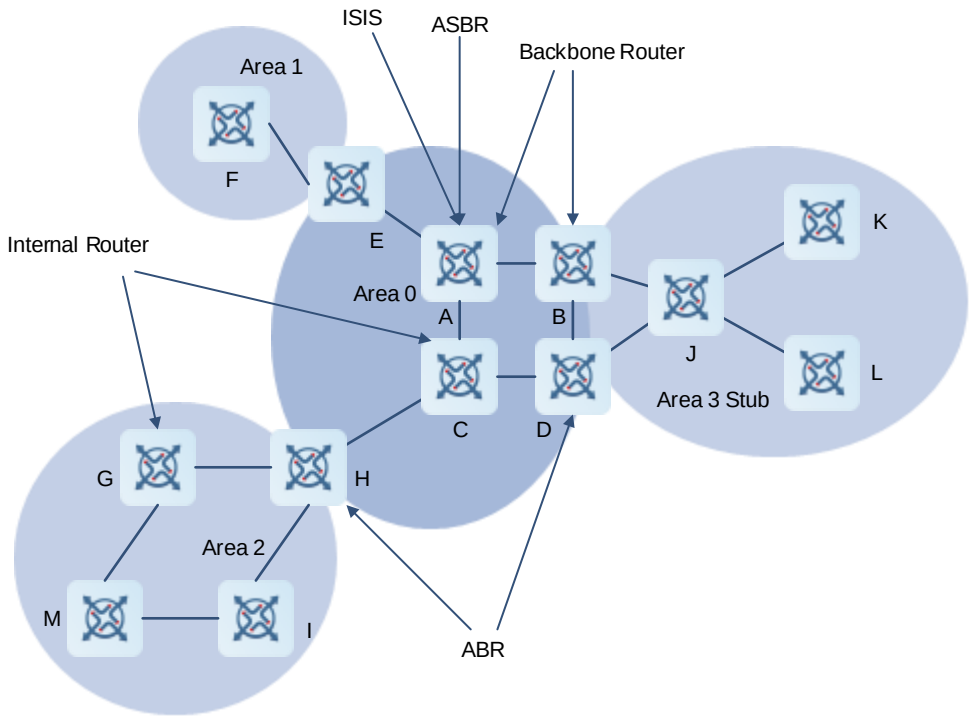
- Totally NSSA

  The relationship between the totally NSSA and NSSA is similar to that between the totally stub area and stub area. The totally NSSA forbids transfer of the Type-3 LSA (inter-domain route) on the basis of NSSA.

Note

- The backbone area cannot be a stub area, totally stub area, NSSA, or totally NSSA.
- The stub area and totally stub area cannot contain any ASBR.
- The stub area, totally stub area, NSSA, and totally NSSA cannot contain any virtual link.

Figure 1-1 OSPF Areas



- OSPF routers

  The following types of routers are defined in OSPF, and assigned with different responsibilities:

  - Internal router

    All interface of an interval router belong to the same OSPF area. See A, C, F, G, I, M, J, K, and L shown in Figure 1-1.

  - ABR

    An ABR is used to connect the backbone area with a normal area. An ABR belongs to two or more areas, and one of the areas must be the backbone area. See B, D, E, and H shown in Figure 1-1.

  - Backbone router

    A backbone router has at least one interface that belongs to the backbone area. All ABRs and all routers in Area 0 are backbone routers. See A, B, C, D, E, and H shown in Figure 1-1.

  - ASBR

    An ASBR is used to exchange routing information with other ASs. An ASBR is not necessarily located on the border of an AS. It may be a router inside an area, or an ABR. See A shown in Figure 1-1.

- OSPF route types

  A mark is displayed in front of each OSPF route to indicate the type of the route. There are six types of OSPF routes:

- O: Internal route

  This type of route describes how to arrive at a destination network in the local area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.

- IA: Inter-area route

  This type of route describes how to arrive at a destination network in another area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.

- E1: Type-1 external route

  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.

- E2: Type-2 external route

  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.

- N1: Type-1 external route of the NSSA

  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA.

- N2: Type-2 external route of the NSSA

  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA.

Note

Reliability of E2 and N2 routes is poor. OSPF believes that the cost of the route from the ASBR to a destination outside an AS is far greater than the cost of the route to the ASBR within the AS. Therefore, when the route cost is computed, only the cost of the route from the ASBR to a destination outside an AS is considered.

- OSPF packets

  OSPF packets are encapsulated in IP packets and transmitted in multicast or unicast mode. When the interfaces running the OSPF process on any network belong to this group, the router running the OSPF process receives all the multicast packets of 224.0.0.5; when the router is used as a DR/BDR on a multi-access network, 224.0.0.6 is used as the multicast receiving address. The OSPF data packet format is shown as follows:

Figure 1-2 OSPF Packet Format

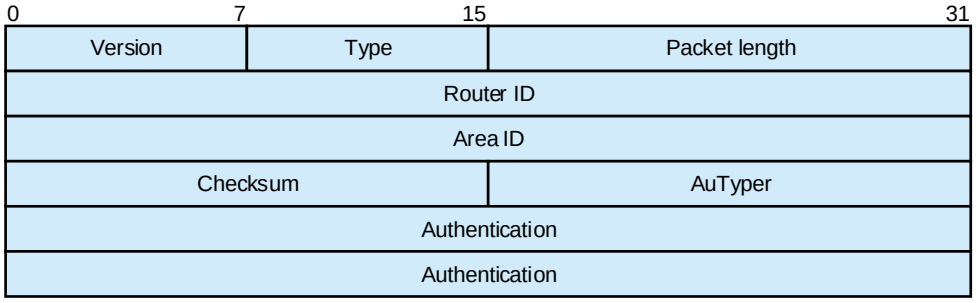


Table 1-1 Description of OSPF Packet Format Fields

Packet Field	Description
Version	Indicates the OSPF version No. The value of OSPFv2 is 2.
Type	Indicates the type of OSPF packet: 1: Indicates hello packet. 2: Indicates DD packet. 3: Indicates LSR packet. 4: Indicates LSU packet. 5: Indicates LSAck packet.
Packet length	Indicates the total length of the OSPF packet including the header, in bytes.
Router ID	Indicates the ID of the router sending the packet.
Area ID	Indicates the area of the router sending the packet.
Checksum	Indicates the checksum of the whole packet excluding the authentication field.
AuType	Indicates the authentication type: 0: Indicates no authentication. 1: Indicates simple authentication. 2: Indicates MD5 authentication.
Authentication	The meaning of this field varies with the authentication type: No authentication: This field is not defined. Simple authentication: This field indicates the password. MD5 authentication: This field includes the key ID, MD5 authentication data length, and sequence number information.

OSPF involves the following five types of packets:

Table 1-2 Types of OSPF Packets

Packet Type	Description
Hello	Hello packets are sent periodically to discover and maintain OSPF neighbor relationships.
DD	DD packets carry brief information about the local LSDB and are used to synchronize the LSDBs between OSPF neighbors.
LSR	LSR packets are used to request the required LSAs from neighbors. LSR packets are sent only after DD packets are exchanged successfully between OSPF neighbors.
LSU	LSU packets are used to send the required LSAs to peers.
LSAck	LSAck packets are used to acknowledge the received LSAs.

- LSA

  OSPF describes the routing information by means of LSA.

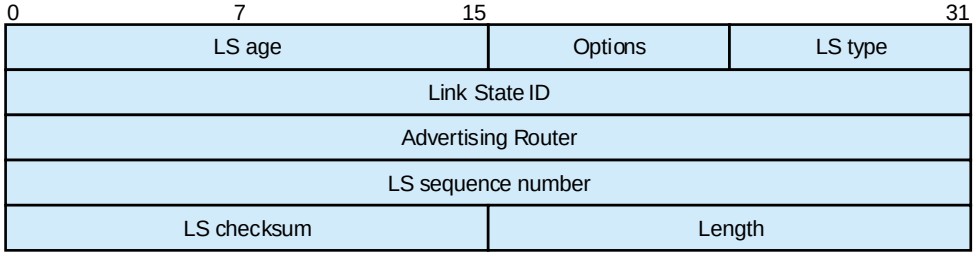
Table 1-3 Types of OSPF LSAs

LSA Type	Description
Router-LSA (Type 1)	This LSA is originated by each router. It describes the link state and cost of the router, and is advertised only within the area where the originating router is located.
Network-LSA (Type 2)	This LSA is originated by a DR on the non-broadcast multiple access (NBMA) network. It describes the link state in the current network segment, and is advertised only within the area where the DR is located.
Network-summary-LSA (Type 3)	This LSA is originated by an ABR. It describes a route to another area, and is advertised to areas except totally stub areas and NSSAs.
ASBR-summary-LSA (Type 4)	This LSA is originated by an ABR. It describes a route to an ASBR, and is advertised to areas except the area where the ASBR is located.
AS-external-LSA (Type 5)	This LSA is originated by an ASBR. It describes a route to a destination outside the AS, and is advertised to all areas except stub areas and NSSAs.
NSSA LSA (Type 7)	This LSA is originated by an ASBR. It describes a route to a destination outside the AS, and is advertised only within the NSSA.

LSA Type	Description
Opaque LSA (Type 9/Type 10/Type 11)	Opaque LSAs provide a generalized mechanism to allow for the future extensibility of OSPF, wherein: ● Type-9 LSAs are advertised only within the network segment where interfaces are located. The grace LSA used to support graceful restart (GR) is one of Type-9 LSAs. ● Type-10 LSAs are advertised within an area. The LSA used to support traffic engineering (TE) is one of Type-10 LSAs. ● Type-11 LSAs are advertised within an AS. At present, there are no application examples of Type-11 LSAs.

Stub areas, NSSAs, totally stub areas, and totally NSSAs are special forms of normal areas and help reduce the number of LSAs transferred in an OSPF area, alleviate the load of routers, and enhance the stability of OSPF routes.

Figure 1-3 LSA Packet Header Format



- OSPF neighbor state

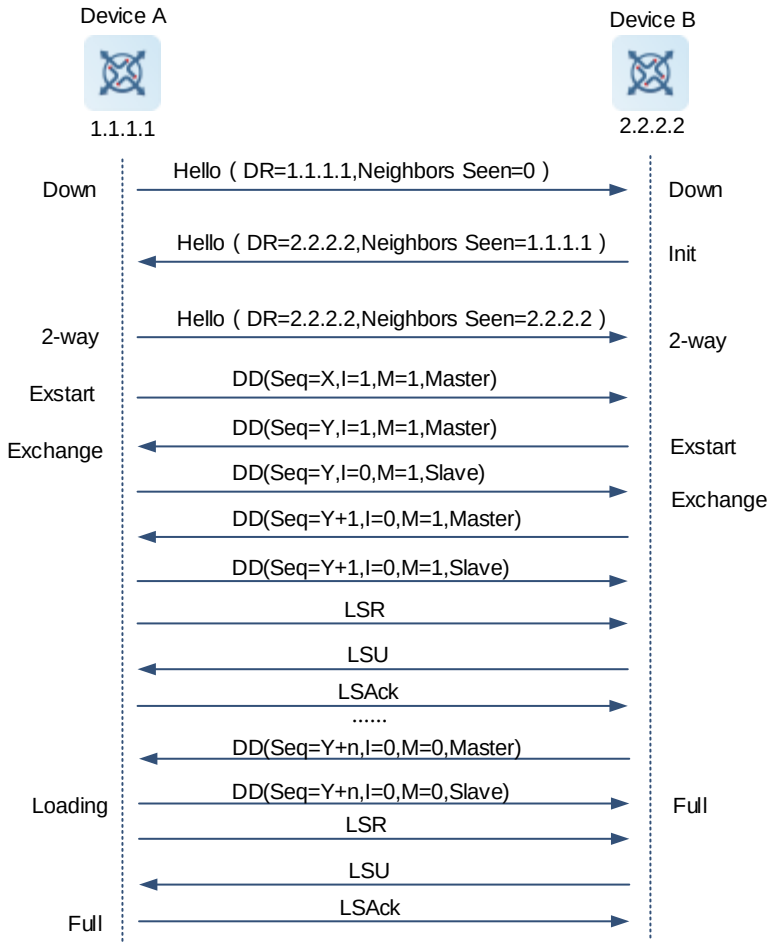
  On the OSPF network, neighbor devices need to reach the adjacency state before exchanging link information. There are several OSPF neighbor states listed below. When a neighbor enters the full state, the adjacency relationship is established. Figure 1-4 shows the adjacency establishment process.

Table 1-4 OSPF Neighbor State Machine and Description

State	Description
Down	The state of the First OSPF neighbor, which indicates that the neighbor's hello packet is not received within the neighbor dead interval.
Attempt	The attempt state router sends a hello packet to the manually configured neighbor periodically. The attempt state applies to the interfaces of NBMA type only.

State	Description
Init	A hello packet has been received from the neighbor, but the packet does not contain the router ID of the neighbor receiving router, that is, the peer end does not receive the hello packet sent by the local end.
Two-Way	Indicates mutual neighbors. ● When the neighbor router ID field in the received hello packet is each other's router ID, and both ends receive the hello packet sent from the peer end, a neighbor relationship is established. ● After this phase ends, DR and BDR will be selected for broadcast and non-broadcast multi-access.
Exstart	Indicates negotiation about the master/slave relationship. ● Selects the initial sequence number for forming an adjacency. ● The master/slave relationship ensures orderly transmission in the subsequent exchange of DD packets.
Exchange	Indicates exchange of DD packets. Checks whether the neighbor can provide new or updated link state information.
Loading	Indicates that, based on the information provided by DBD, the router will send LSR and interactive LSU to implement synchronization with LSDB.
Full	Indicates establishment of an adjacency. Indicates that the LSDBs of the two devices have been synchronized, and the adjacency state has been established between the local device and the neighbor device.

Figure 1-4 OSPF Adjacency Establishment Process on Broadcast Network



- OSPF network types

  A router does not necessarily need to exchange LSAs with every neighbor or set up an adjacency with every neighbor. To improve efficiency, OSPF classifies networks that use various link layer protocols into five types so that LSAs are exchanged in different ways to set up an adjacency.

  By default, Ethernet and fiber distributed data interface (FDDI) belong to the broadcast type, X.25, frame relay, and ATM belong to the NBMA type, and PPP, HDLC, and LAPB belong to the P2P type.

Table 1-5 Introduction to OSPF Network Types

Network Type	Link Layer Protocol	Neighbor Relationship and DR Election
Broadcast	Ethernet and FDDI belong to the broadcast network type by default.	● Neighbors are discovered, and the DR and BDR are elected. ● The DR or BDR exchanges LSAs with all other routers to set up an adjacency. ● Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.
NBMA	X.25, frame relay, and ATM belong to NBMA networks by default.	● Neighbors are manually configured, and the DR and BDR are elected. ● The DR or BDR exchanges LSAs with all other routers to set up an adjacency. ● Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.
Point-to-Point (P2P)	PPP, HDLC, and LAPB belong to the P2P network type by default.	● Neighbors are automatically discovered, and the DR or BDR is not elected. ● LSAs are exchanged between routers at both ends of the link, and the adjacency is set up.
Point-to-Multipoint (P2MP)	Networks without any link layer protocol belong to the P2MP network type by default.	● Neighbors are automatically discovered, and the DR or BDR is not elected. ● LSAs are exchanged between any two routers, and the adjacency is set up.
P2MP broadcast	Networks without any link layer protocol belong to the P2MP network type by default.	● Neighbors are manually configured, and the DR or BDR is not elected. ● LSAs are exchanged between any two routers, and the adjacency is set up.

- DR and BDR

  On the broadcast or NBMA network, many unwanted LSAs will be created when an adjacency is set up with related routers. If there are n routers, n*(n-1)/2 adjacency relationships will be set up, and n^2 LSAs will be generated on the network. In the process of setting up the adjacency and exchanging LSAs, many unwanted copies will be produced, which leads to chaos in the flooding of a multi-access network. To avoid these problems on a multi-access network, OSPF defines the concepts of DR and BDR.

After the DR and BDR are elected, all routers will set up an adjacency relationship with the DR and BDR only, send information to the DR/BDR, and the DR will broadcast the network link state. The routers other than DR and BDR are called DR Other. DR Other will no longer set up an adjacency relationship or exchange any routing information with each other, thus reducing the number of adjacency relationships between routers on the broadcast and NBMA networks, as shown in Figure 1-5 and Figure 1-6.

Figure 1-5 Number of Adjacency Relationships Before DR Election

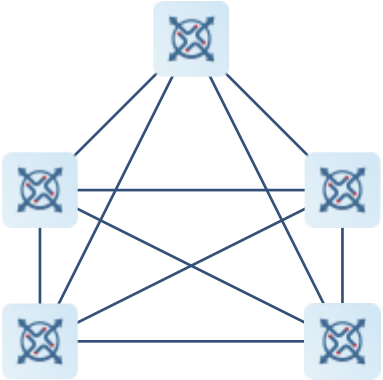
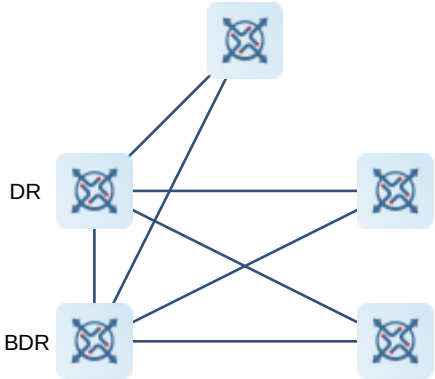


Figure 1-6 Number of Adjacency Relationships After DR Election

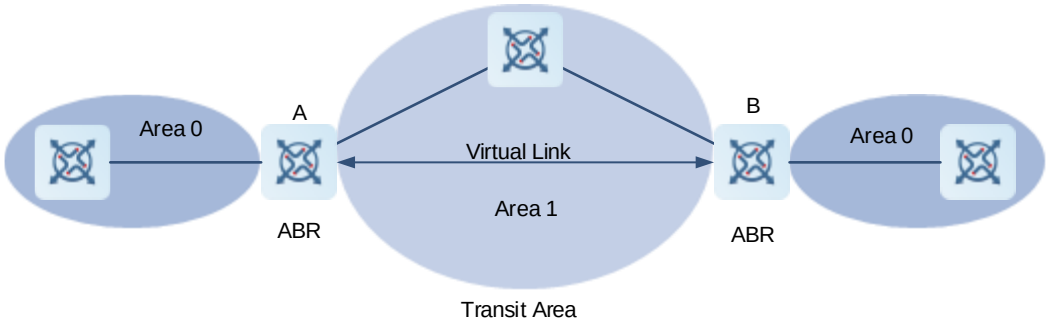


- Virtual link

  OSPF supports virtual links. A virtual link is a logical link that belongs to the backbone area. It is used to resolve the problems such as a discontinuous backbone area or a failure to directly connect a normal area to the backbone area on the physical network. A virtual link supports traversal of only one normal area, and this area is called transit area. Routers on both ends of a virtual link are ABRs.

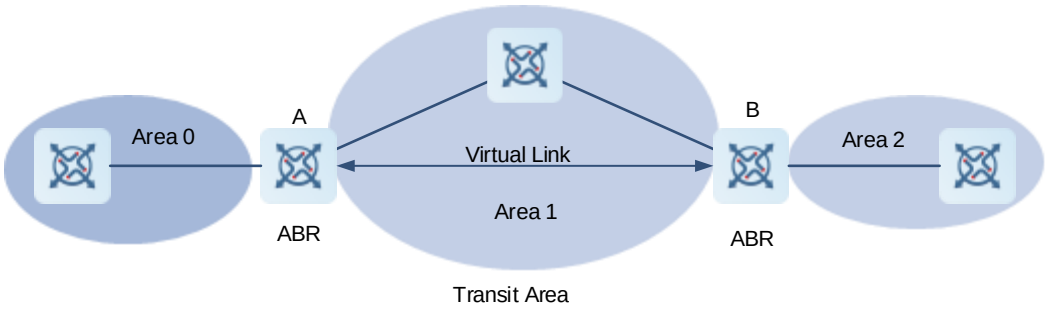
  A virtual link relies on an OSPF intra-domain route, making two ABRs adjacent. The OSPF packet information exchanged by ABRs is transparent to the intermediate device.

Figure 1-7 Discontinuous Backbone Area on the Physical Network



As shown in Figure 1-7, a virtual link is set up between A and B to connect to Area 0. Area 1 is a transit area, and A and B are ABRs of Area 1.

Figure 1-8 Failure to Directly Connect a Normal Area to the Backbone Area on the Physical Network



As shown in Figure 1-8, a virtual link is set up between A and B to extend Area 0 to B so that Area 0 can be directly connected to Area 2 on B. Area 1 is a transit area, A is an ABR of Area 1, and B is an ABR of Area 1 and Area 2.

3. OSPF Routing

- Route cost

  If redundancy links or devices exist on the network, multiple paths may exist from the local device to the destination network. OSPF selects the path with the minimum total cost to form an OSPF route. The total cost of a path is equal to the sum of the costs of individual links along the path. The total cost of a path can be minimized by modifying the costs of individual links along the path. In this way, OSPF selects this path to form a route.

  With configuration commands, you can modify the following link costs:

  - Cost from an interface to a directly connected network segment and cost from the interface to a neighbor.
  - Cost from an ABR to the inter-area summarization network segment and cost from the ABR to the default network segment.
  - Cost from an ASBR to an external network segment and cost from the ASBR to the default network

segment.

Note

Cost value refers to the cost of a link and the link quality value after calculation. Metric is the cost of a complete path and the total cost of the links passed.

- OSPF management distance

  The management distance (AD) evaluates reliability of a route. Its value is an integer ranging from 0 to 255. A smaller AD value indicates that the route is more trustworthy. If multiples exist to the same destination, the route preferentially selects a route with a smaller AD value. The route with a greater AD value becomes a floating route, that is, a standby route of the optimum route.

  By default, the route coming from one source corresponds to an AD value. The AD value is a local concept. Modifying the AD value affects route selection only on the current router.

Table 1-6 Routing Protocols and Default Management Distances

Route Source	Directly-connected network	Static route	EBGP route	OSPF route	IS-IS route	RIP route	IBGP route	Unreachable route
Default AD	0	1	20	110	115	120	200	255

4. OSPF Route Advertisement

- Route redistribution

  Route redistribution refers to the process of introducing routes of other routing protocols, routes of other OSPF processes, static routes, and direct routes that exist on the device to an OSPF process so that these routes can be advertised to neighbors using Type-5 and Type-7 LSAs. A default route cannot be introduced during route redistribution.

  Route redistribution is often used for interworking between ASs. You can configure route redistribution on an ASBR to advertise routes outside an AS to the interior of the AS, or routes inside an AS to the exterior of the AS.

- Default route introduction

  By configuring a command on an ASBR, you can introduce a default route to an OSPF process so that the route can be advertised to neighbors using Type 5 and Type 7 LSAs.

  Default route introduction is often used for interworking between ASs. One default route is used to replace all the routes outside an AS.

5. OSPF Route Summarization

Route summarization is a process of summarizing routing information with the same prefix into one route, and advertising the summarized route to neighbors by replacing a large number of individual routes. Route summarization helps reduce the protocol interaction load and the size of the routing table.

By default, the ABR advertises inter-area routing information by using Type-3 LSAs within a network segment, and advertises redistributed routing information by using Type-5 and Type-7 LSAs. If continuous network segments exist, you are advised to configure route summarization.

When configuring route summarization, the summarization range may exceed the actual network scope of routes. If the data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, ABR or ASBR will automatically add a discard route to the routing table. This route will not be advertised.

6. OSPF Route Filtering

OSPF allows filtering of the learned and exchanged routes and LSAs so as to meet the security requirements in specific scenarios, for example, the routes of some network segments are not intended to be learned by other areas.

With configuration commands, you can configure route filtering for the following items:

- Interface: The interface is prevented from sending any LSAs or exchanging any LSAs with neighbors.
- Routing information advertised between areas: Only the Type-3 LSA that meets the filtering conditions can be advertised to another area.
- Routing information outside an AS: Only the Type-5 and Type-7 LSAs that meet the filtering conditions can be redistributed to the OSPF process.
- LSAs received by a router: In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

7. Stub Area and NSSA

The stub/totally stub area and NSSA/totally NSSA help reduce the protocol interaction load and the size of the routing table.

- If an appropriate area is configured as a stub/totally stub area or NSSA/totally NSSA, advertisement of a large number of Type-5 and Type-3 LSAs can be avoided within the area.

Table 1-7 LSAs in Stub Area/NSSA

Area	Types 1 and 2	Type 3	Type 4	Type 5	Type 7
Non-stub/totally stub area and non-NSSA/totally NSSA	Allowed	Allowed	Allowed	Allowed	Not allowed
Stub area	Allowed	Allowed (containing one default route)	Not allowed	Not allowed	Not allowed

Area	Types 1 and 2	Type 3	Type 4	Type 5	Type 7
Totally stub area	Allowed	Only one default route is allowed.	Not allowed	Not allowed	Not allowed
NSSA	Allowed	Allowed (containing one default route)	Allowed	Not allowed	Allowed
Totally NSSA	Allowed	Only one default route is allowed.	Allowed	Not allowed	Allowed

Note

The ABR uses Type-3 LSAs to advertise a default route to the stub/totally stub area or NSSA/totally NSSA.

The ABR converts Type-7 LSAs in the NSSA/totally NSSA to Type-5 LSAs, and advertises Type-5 LSAs to the backbone area.

- If an appropriate area is configured as a stub/totally stub area or NSSA/totally NSSA, a large number of E1, E2, and IA routes will not be added to the routing table of a router in the area.

Table 1-8 Route Types in Stub Areas/NSSAs

Area	Routes Available in the Routing Table of a Router Inside the Area
Non-stub/totally stub area and non-NSSA/totally NSSA	O: a route to a destination network in the local area IA: a route to a destination network in another area E1 or E2: a route or default route to a destination network segment outside the AS (via any ASBR in the AS)
Stub area	O: a route to a destination network in the local area IA: a route or a default route to a destination network in another area
Totally stub area	O: a route to a destination network in the local area IA: a default route
NSSA	O: a route to a destination network in the local area IA: a route or a default route to a destination network in another area N1 or N2: a route or default route to a destination network segment outside the AS (via an ASBR in the local area)

Area	Routes Available in the Routing Table of a Router Inside the Area
Totally NSSA	O: a route to a destination network in the local area IA: a default route N1 or N2: a route or default route to a destination network segment outside the AS (via an ASBR in the local area)

8. Enhanced Security and Reliability

The functions such as authentication and bidirectional forwarding detection (BFD) correlation are used to enhance security, stability, and reliability of OSPF.

- Authentication

  Authentication prevents routers that illegally access the network and hosts that forge OSPF packet from participating in the OSPF process. OSPF packets received on the OSPF interface or at both ends of the virtual link are authenticated. If authentication fails, the packets are discarded and no adjacency can be set up.

  Enabling authentication can avoid learning unauthenticated or invalid routes, thus preventing advertising valid routes to unauthenticated devices. On the broadcast-type network, authentication also prevents unauthenticated devices from becoming designated devices, ensuring stability of the routing system and protecting the routing system against intrusions.

  Authentication is classified into following two types:

  - Area authentication: This area-level authentication authenticates the packets transmitted by all the interfaces in the area. This type is configured in OSPF routing process mode.
  - Interface authentication: This neighbor-level authentication authenticates the packets transmitted on the related interface. This type is configured in interface mode.

- MTU verification

  Upon receiving a DD packet, OSPF checks whether the MTU of the neighbor interface is the same as that of the local interface. If the MTU of the interface specified in the received DD packet is greater than that of the interface that receives the packet, the adjacency cannot be set up. Disabling MTU verification can avoid this problem.

- Source address verification

  Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information will be notified during the P2P link negotiation process, OSPF checks whether the source address of the packet is the address advertised by the peer during negotiation. If not, OSPF determines that the packet is invalid and discards this packet. In particular, OSPF never verifies the address of an interface not configured with an IP address.

In some scenarios, the source address of a packet received by OSPF may not be in the same network segment as the receiving interface, so the OSPF address verification fails. For example, the negotiated peer address cannot be obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

- Two-way maintenance

  OSPF routers periodically send hello packets to each other to maintain the adjacency. On a large network, a lot of packets may be sent or received, occupying a great proportion of CPU and memory. As a result, some packets are delayed or discarded. If the processing time of hello packets exceeds the neighbor dead interval, the adjacency will be destroyed.

  If the two-way maintenance function is enabled, in addition to the hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors, which makes the adjacency more stable.

- Concurrent neighbor interaction restriction

  When a router simultaneously exchanges data with multiple neighbors, its performance may be affected. If the maximum number of neighbors that concurrently initiate or accept interaction with the OSPF process is restricted, the router can interact with neighbors by batches, which ensures data forwarding and other key services.

- Overflow

  OSPF requires that routers in the same area store the same LSDB. The number of routers keeps increasing on the network. Some routers, however, cannot store so much routing information due to the limited system resources. The large amount of routing information may exhaust the system resources of routers, causing failures of the routers.

  The overflow function limits the number of external routes in the LSDB to control the size of the LSDB.

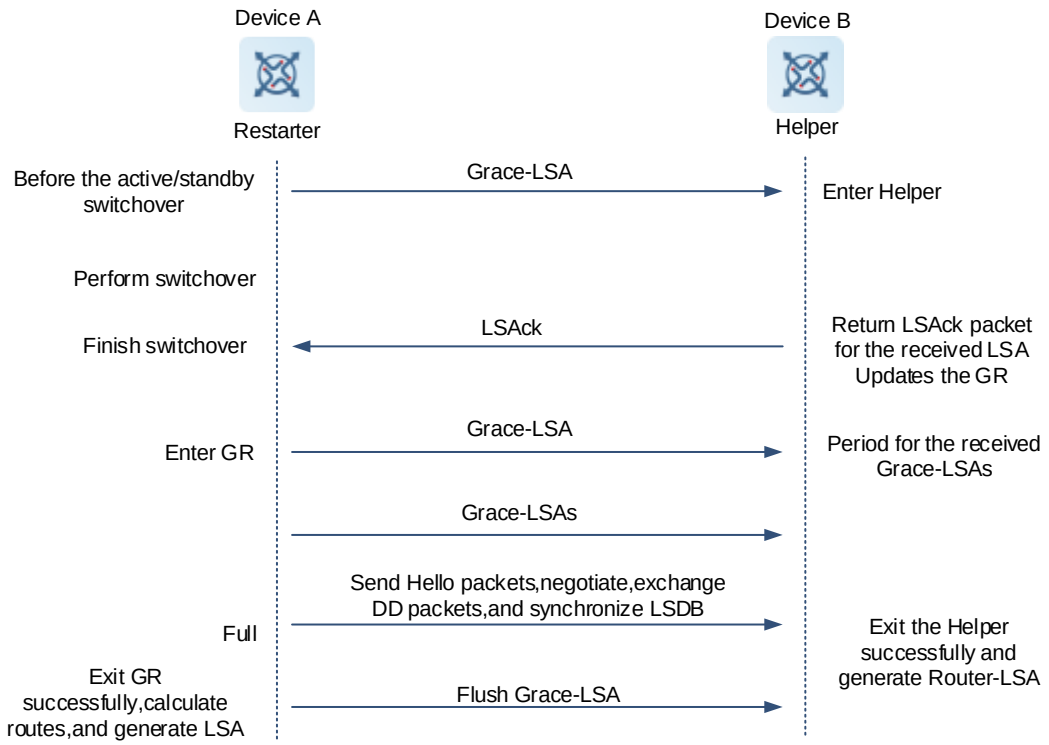
  When the number of external routes on a router exceeds the upper limit, the router enters the overflow state. The router deletes the external routes generated by itself from the LSDB, and does not generate new external routes. In addition, the router discards the newly received external routes. After the overflow state timer (5s) expires, if the number of external routes is lower than the upper limit, the normal state is restored.

- GR

  The control and forwarding separated technology is widely used among routers. On a relatively stable network topology, when a GR-enabled router is restarted on the control plane, data forwarding can continue on the forwarding plane. In addition, actions (such as adjacency re-forming and route computation) performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

  Currently, the GR function is used only during active/standby switchover and system upgrade.

Figure 1-9 Normal OSPF GR Process



- The GR process requires collaboration between the restarter and the helper. The restarter is the router where GR occurs. The helper is a neighbor of the restarter.
- When entering or exiting the GR process, the restarter sends a grace-LSA to the neighbor, notifying the neighbor to enter or exit the helper state.
- When the adjacency between the restarter and the helper reaches the full state, the router can exit the GR process successfully.

- NSR

  During nonstop routing (NSR), OSPF-related information is backed up from the active supervisor module of a distributed device to the standby supervisor module, or from the active host of a virtual switching unit (VSU) to the standby host. In this way, the device can automatically recover the link state and re-generate routes without the help of the neighbor devices during the active/standby switchover. The specific information of NSR active/standby synchronization includes configuration information backup, process information backup, interface information backup, neighbor information backup, and LSA information backup.

- Fast hello correlation with BFD and fast reroute

  After a link fails, it takes a period of time (about 40s) before OSPF can sense the failure of the neighbor. Then, OSPF advertises the information and re-computes the SPT. During this period, traffic is interrupted.

  - After the fast hello function is enabled (that is, the neighbor dead interval is set to 1s), OSPF can sense the failure of the neighbor within 1s once a link is faulty. This greatly accelerates route convergence and

prevents traffic interruption.

- BFD is used to test connectivity between devices. A link fault can be detected in as short as 150 ms. After OSPF is correlated with BFD, OSPF can sense the failure of a neighbor in as short as 150 ms once a link is faulty. This greatly accelerates route convergence and prevents traffic interruption.
- Fast reroute prepares a backup route for OSPF. Once the OSPF senses the failure of a neighbor, the traffic is immediately switched over to the standby route, thus preventing traffic interruption.

- iSPF feature
  - The OSPF topology is area based. The SPF algorithm is run for independent computation in each area. The standard SPF algorithm re-computes the topology of the entire area each time even if only the leave nodes change in the area topology.
  - When computing the network topology, the incremental shortest path first (iSPF) method corrects only the nodes on the SPT that are affected by the topology changes, and does not re-build the entire SPT. This can effectively ease the pressure on the router processors on a large network, especially when the network is not stable.
- Fast convergence

  When a link or a router on the OSPF network fails, the packets that need to be transmitted through the faulty link or the faulty router to reach the destination will be lost or cause a routing loop, and the data traffic will be interrupted. The interrupted traffic cannot resume normal transmission until OSPF completes convergence according to the new topology network.

  To minimize the traffic interruption time caused by a network failure, the administrator can configure the OSPF fast reroute or fast hello function to speed up network convergence.

9. Network Management Functions

Functions such as management information base (MIB) and Syslog are used to facilitate OSPF management.

- MIB

  MIB is the device state information set maintained by a device. You can use the management program to view and set the MIB node.

  Multiple OSPF processes can be simultaneously started on a router, but the OSPF MIB can be bound to only one OSPF process.
- Trap

  A trap message is a notification generated when the system detects a fault. This message contains the related fault information.

  If the trap function is enabled, the router can actively send the trap messages to the network management device.
- Syslog

  The syslog records the operations (such as command configuration) performed by users on routers and specific events (such as network connection failures).

If the syslog is allowed to record the adjacency changes, the network administrator can view the logs to learn the entire process that the OSPF adjacency is set up and maintained.

10. VPN Extended Feature of OSPF

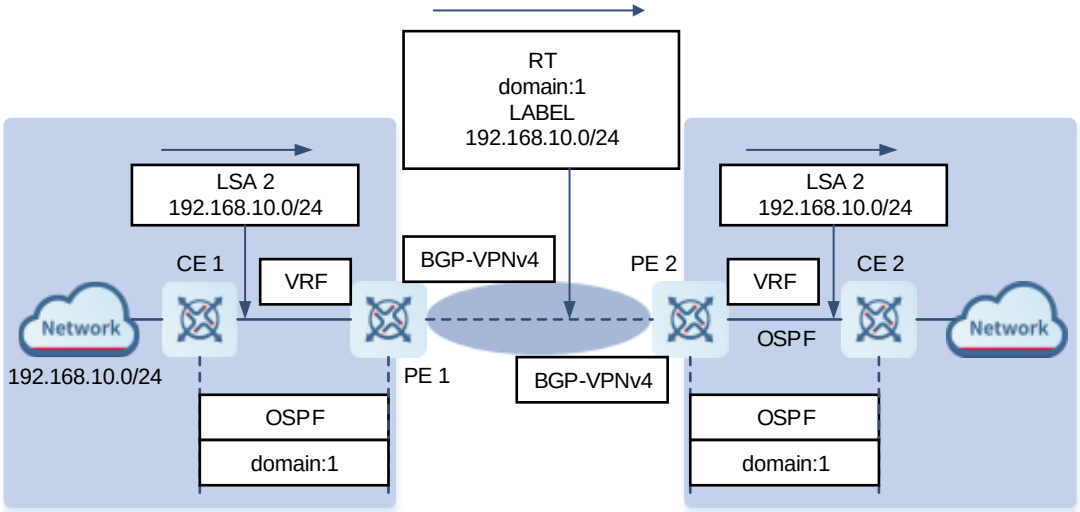
OSPF is a widely used IGP. In most of the existing application solutions, OSPF is generally selected as an internal routing protocol for VPN users. If OSPF is also used between PEs and CEs, other routing protocols are not needed, which simplifies the configuration and management of CEs.

- Domain ID

  A domain ID refers to the ID of an OSPF domain to which a route belongs. When a CE learns an OSPF route in a VPN internal site, and this route is advertised to a PE as a Type-1/2/3 LSA, and is redistributed to the Border Gateway Protocol (BGP) domain and converted into a VPN route, the domain ID is also redistributed to the BGP domain along with the route. Then, this domain is also advertised as the extcommunity attribute of the VPN route. When another PE receives this VPN route and redistributes it to a VRF OSPF process, the domain ID is redistributed to the VRF OSPF process along with the route. If the VRF OSPF process confirms that the domain ID in the route is the same as that in the local VRF OSPF process, it advertises the route to the CE as an internal route. If the VRF OSPF process confirms that the domain ID in the route is different from that in the local VRF OSPF process, the VRF OSPF process advertises the route to the CE as an external route.

  As shown in Figure 1-10, for internal routes belonging to the same OSPF domain, CE1 advertises the routes to PE1 as Type-2 LSAs, which are converted into VPN routes and advertised to PE2. After receiving the routes, PE2 redistributes them to the VRF OSPF process. The domain IDs in the VRF OSPF process are the same as those of the VPN routes, and therefore, the VPN routes are advertised to the VPN site as internal routes.

Figure 1-10 Diagram of Domain ID



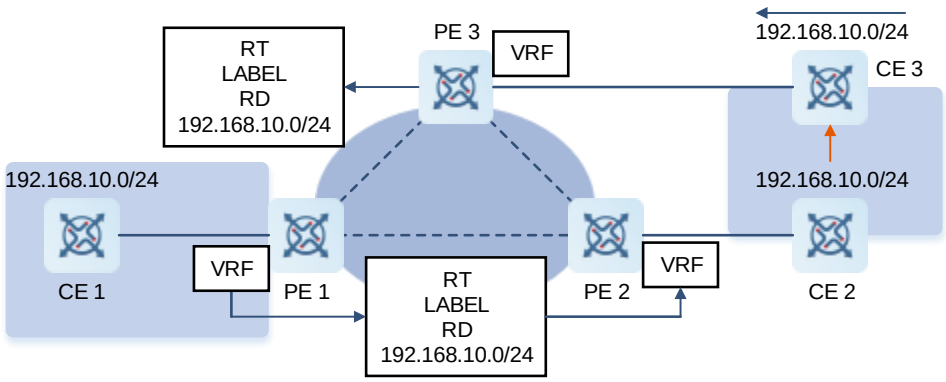
- DN bit technology

  The DN bit is a loop detection technology running the OSPF protocol between a PE and a CE. In some scenarios, loops may arise when OSPF runs between a PE and a CE, for example, multiple CEs are connected

to one VPN site. If one PE advertises learned VPN routes to the VPN site, and the VPN site advertises the routes to another PE via OSPF, a loop may occur.

As shown in Figure 1-11, PE1 advertises the 192.168.10.0/24 route to PE2 and PE3, CE2 advertises the route to CE3 via OSPF, and CE3 advertises the route to PE3, which redistributes the route to the BGP domain of PE3. PE3 selects the route that is redistributed via OSPF and converts this route into a VPNv4 route for advertisement. As a result, a loop may occur.

Figure 1-11 Diagram of DN Bit Technology



For this, when a PE advertises a Type-3/5/7 LSA to a CE, the DN bit is set to ON in the optional field of the LSA, to prevent possible loops. When an LSA received by another PE contains the DN bit in the optional field, the OSPF of the PE will not use this LSA for OSPF calculation.

- VPN router tag

  Router-tag is another loop detection technology running OSPF between a PE and a CE. When OSPF runs between a PE and a CE, the VRF OSPF process of the PE has a router tag by default, which is called VPN router tag. When a VPN route is imported into the VRF OSPF process of a PE and is converted into a Type-5/7 LSA and advertised to a CE, the LSA carries the VPN router-tag. When multiple PEs are connected to one VPN site, if the Type-5/7 LSA received by a PE contains the VPN router tag and the VPN router tag is the same as the VPN router tag of the OSPF process, the LSA will not be used for OSPF route calculation.

- Area deployment

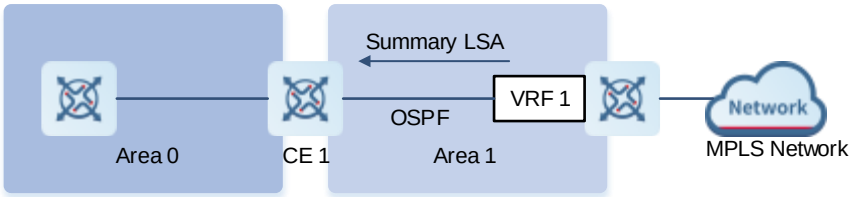
  In normal cases, links between a PE and a CE may belong to any OSPF area. If links between a PE and a CE belong to a non-zero area, the PE is an ABR for the OSPF area where the CE resides. This may cause problems because the ABR running OSPF has the following features:

  - The ABR calculates Type-3 LSAs in the backbone area only.
  - The ABR forwards only Type-3 LSAs in the backbone area to a non-backbone area.

  As shown in Figure 1-12, if the link between a PE and a CE belongs to a non-zero area, the PE redistributes the VPNv4 routes advertised by Multiprotocol Extensions for BGP (MP-BGP) to the OSPF domain, restores them to type-3 LSAs, and advertises them to CE1. CE1 does not calculate LSAs in non-backbone areas. Therefore, these LSAs are not advertised to routers in Area 0 and the VPN internal sites cannot learn routes of other sites.

Therefore, exercise caution during the deployment when the links between a PE and a CE belong to a non-zero area.

Figure 1-12 Diagram of Area Deployment

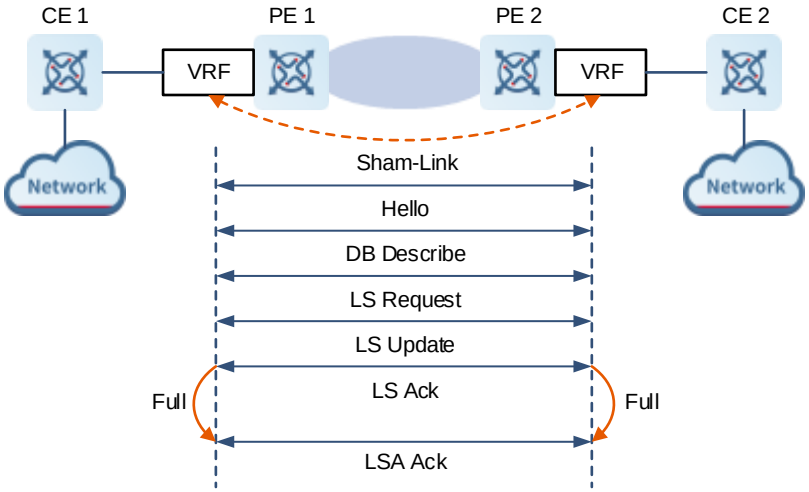


In L3VPN application, if OSPF is run between a PE and a CE to exchange VPN routes, do not deploy the backbone area at VPN internal sites if possible. If a router at a VPN internal site belongs to a backbone area in addition to a PE, at least one router series product at the VPN internal site must be connected to the PE and the links between the CE and PE must belong to Area 0. In this way, inter-area routes and external routes can be transmitted between the PE and the VPN site.

- Sham link

  The sham link is not a real link but a virtual link established between VRF instances of two PEs. Like a normal OSPF link, a sham link has its OSPF interfaces, and is capable of sending OSPF protocol packets, establishing neighbor relationships, and sending LSAs. When LSAs are flooded on a sham link, no types of the OSPF routes will change, as shown in Figure 1-13.

Figure 1-13 Diagram of Sham Link



The purposes of establishing sham-links between VRF OSPF processes of different PEs are as follows:

- When the Multiprotocol Interior Border Gateway Protocol (MP-IBGP) is used to carry private routes, it only transfers routes; after the routes reach the peer PE and restored, MP-IBGP imports the original OSPF routes in a best-effort manner, and the OSPF topology information cannot be communicated properly. With

sham-link, an OSPF link can be established to implement actual interworking between OSPF processes at each site and establish a complete topology.

- Different sites in the same VPN exchange information via the MPLS backbone network. One link is connected between these VPN sites. The purpose of this link is that VPN sites can communicate with each other through this link when the MPLS backbone network is unavailable. This link is called backdoor link.

If two VPN sites belong to the same OSPF area and one backdoor link is connected in between, routes inside the two sites are exchanged through both the MPLS backbone network and the backdoor link. Routes exchanged through the MPLS backbone network are inter-domain routes while routes exchanged through the backdoor link are intra-domain routes. The intra-domain routes advertised by the backdoor link are prior to the inter-domain routes advertised by the MPLS backbone network. Therefore, the forwarding of the routes inside the two sites takes the backdoor link first, which is against the intention of backdoor link connection for VPN users. In this case, a sham link is also required.

1.1.3 Protocols and Standards

- RFC2328: OSPF Version 2
- RFC2370: This memo defines enhancements to the OSPF protocol to support a new class of link-state advertisements (LSA) called Opaque LSAs. Opaque LSAs provide a generalized mechanism to allow for the future extensibility of OSPF.
- RFC3137: This memo describes a backward-compatible technique that may be used by OSPF (Open Shortest Path First) implementations to advertise unavailability to forward transit traffic or to lower the preference level for the paths through such a router.
- RFC3623: This memo documents an enhancement to the OSPF routing protocol, whereby an OSPF router can stay on the forwarding path even as its OSPF software is restarted.
- RFC3630: This document describes extensions to the OSPF protocol version 2 to support intra-area Traffic Engineering (TE), using Opaque Link State Advertisements.
- RFC3682: The use of a packet's Time to Live (TTL) (IPv4) or Hop Limit (IPv6) to protect a protocol stack from CPU-utilization based attacks has been proposed in many settings.
- RFC3906: This document describes how conventional hop-by-hop link-state routing protocols interact with new Traffic Engineering capabilities to create Interior Gateway Protocol (IGP) shortcuts.
- RFC4576: This document specifies the necessary procedure, using one of the options bits in the LSA (Link State Advertisements) to indicate that an LSA has already been forwarded by a PE and should be ignored by any other PEs that see it.
- RFC4577: This document extends that specification by allowing the routing protocol on the PE/CE interface to be the Open Shortest Path First (OSPF) protocol.
- RFC4750: This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for managing version 2 of the Open Shortest Path First Routing Protocol. Version 2 of the OSPF protocol is specific to the IPv4 address family.

1.2 Configuration Task Summary

The OSPFv2 configuration includes the following tasks:

(1) Configuring Basic Features

- a Configuring OSPF Process
- b (Optional) Configuring Router ID
- c Adding Interface IP to OSPF and Specifying Area ID
- d Enabling OSPF on an Interface and Specifying an Area ID
- e (Optional) Creating a Virtual Link

(2) Configuring OSPF Network Type

- a Configuring the Interface Network Type
- b (Optional) Configuring a Neighbor
- c (Optional) Configuring the Interface Priority
- d (Optional) Disabling Source Address Verification

(3) Adjusting OSPF Routing

- Configuring the AD
- Configuring the Reference Bandwidth
- Configuring the Cost of an Interface
- Configuring Cost Fallback Value for an AP
- Configuring the Cost of the Default Route in a Stub Area or an NSSA
- Configuring the Default Metric Value for Redistribution Value
- Configuring the Maximum Metric
- Configuring RFC1583 Compatibility
- Configuring Association of External Route Forwarding Addresses with Interface Configuration

(4) Configuring OSPF Route Advertisement

- a Configuring External Route Redistribution
- b Generating a Default Route
- c (Optional) Configuring a Device as ASBR

(5) Configuring OSPF Route Summarization

- a Configuring Inter-Area Route Summarization
- b Configuring External Route Summarization
- c Configuring a Discard Route

(6) Configuring OSPF Route Filtering

- Configuring a Passive Interface

- Configuring LSA Update Packet Filtering
- Configuring Inter-area Route Filtering
- Configuring Redistributed Route Filtering
- Configuring Learned Route Filtering

(7) Adjusting OSPF Network Convergence Speed

- Configuring the Hello Interval
- Configuring the Dead Interval
- Configuring LSU Transmission Delay
- Configuring LSU Retransmission Interval
- Configuring LSU Generation Time
- Configuring LSA Group Refresh Time
- Configuring LSA Group Refresh Interval
- Configuring Duplicate LSA Receiving Delay
- Configuring Inter-Area Route Computation Delay
- Configuring External Route Computation Delay
- Configuring SPF Computation Delay
- Enabling Two-Way Maintenance

(8) Configuring Stub Area and NSSA

- Configuring a Stub Area
- Configuring an NSSA

(9) Configuring OSPF Authentication

- Configuring the Authentication Type of an Area
- Configuring the Authentication Type of an Interface
- (Optional) Configuring a Plain Text Authentication Key for an Interface
- (Optional) Configuring an MD5 Authentication Key for an Interface

(10) Enabling Fast Reroute

a Configuring Fast Reroute

b Configuring Interface LFA Protection

c Preventing an Interface From Becoming a Backup Interface

(11) Modifying the Maximum Number of Concurrent Neighbors

- Configuring the Maximum Number of Concurrent Neighbors on the Current Process
- Configuring the Maximum Number of Concurrent Neighbors on All Processes

(12) Configuring the GR Function

a Enabling the GR Function

b Configuring the OSPF GR Helper Function

(13) Correlating OSPF with BFD

- Configuring BFD Correlation with OSPF on an Interface
- Configuring BFD Correlation with OSPF Globally

(14) Enabling Overflow

- Configuring the Memory Overflow Function
- Configuring the Database Overflow Function
- Configuring the External LSA Database Overflow Function

(15) Configuring VPN Extended Feature of OSPF

- (Optional) Configuring Domain ID
- (Optional) Configuring a Sham Link
- (Optional) Configuring a Domain Label
- (Optional) Disabling Loop Detection for a VRF OSPF Process
- (Optional) Configuring Extcommunity Attribute for a VPN Route
- Disabling Loop Detection Using the DN Bit of LSA
- Disabling Loop Detection Using the Route Tag of LSA

(16) Configuring Network Management Functions

- Binding the MIB with an OSPF Process
- Configuring the Trap Function
- Configuring the Logging Function

(17) Enabling NSR

(18) Enabling the iSPF Feature

(19) Configuring to Disable MTU Verification

(20) Configuring a Super VLAN to Enable OSPF

1.3 Configuring Basic Features

1.3.1 Overview

Set up an OSPF routing domain on the network to provide IPv4 unicast routing service for users on the network.

1.3.2 Restrictions and Guidelines

- Ensure that the IP unitcast routing function is enabled, that is, **ip routing** is not disabled; otherwise, OSPF cannot be enabled.
- You are strongly advised to manually configure the router ID.
- After **ip ospf disable all** is configured, the interface neither sends or receives any OSPF packet, nor participates

in OSPF computation even if the interface belongs to the advertisement range of the **network** command.

1.3.3 Configuration Tasks

The basic function configuration of OSPF includes the following tasks:

(1) Configuring OSPF Process

(2) (Optional) Configuring Router ID

(3) Adding Interface IP to OSPF and Specifying Area ID

(4) Enabling OSPF on an Interface and Specifying an Area ID

(5) (Optional) Creating a Virtual Link

1.3.4 Configuring OSPF Process

1. Overview

Configure and enable an RIP process.

2. Restrictions and Guidelines

- OSPF supports multiple instances, and each instance corresponds to an OSPF process. One or more OSPF processes can be started on a router. Each OSPF process runs OSPF independently, and the processes are mutually isolated.
- The process ID takes effect only on the local router, and does not affect exchange of OSPF packets on adjacent interfaces.
- This configuration must be performed on every router that requires OSPF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an OSPF process and enter OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

1.3.5 Configuring Router ID

1. Overview

Router ID is the unique identifier of a router in the OSPF domain, so the router ID must be unique on the entire network; otherwise it will lead to problems such as abnormality in neighbor relationship establishment and routing information error. Moreover, different OSPF processes in the same router need to use different router IDs.

2. Restrictions and Guidelines

- You are strongly advised to manually configure the router ID.
- When no router ID is configured, OSPF selects an interface IP address. If no IP address is configured for any interface, or the configured IP addresses have been used by other OSPF processes, you must manually configure the router ID.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure a router ID.

router-id *router-id*

By default, the OSPF routing process elects the largest IP address among all the loopback interfaces as the router ID. If the loopback interfaces configured with IP addresses are not available, the OSPF process elects the largest one among the IP addresses of all its physical interfaces as the router ID.

1.3.6 Adding Interface IP to OSPF and Specifying Area ID

1. Overview

Add an interface to the OSPF area and associate it with the area. An interface can be associated with only one area and needs to be configured on all the OSPF-enabled routers.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Add an interface IP address to the OSPF area and specify an area ID.

network *ipv4-address wildcard* **area** *area-id*

No interface IP address is configured to join the OSPF area by default.

1.3.7 Enabling OSPF on an Interface and Specifying an Area ID

1. Overview

Running this command will add all IP addresses on the interface to the OSPF process.

2. Restrictions and Guidelines

- The configuration is mandatory for every OSPF-enabled router.
- You can also add an interface to OSPF process using the **network** command on the instance. If two commands are run at the same time, the configuration on the interface takes effect first.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable OSPF on an interface and specify an area ID.

ip ospf *process-id* **area** *area-id*

OSPF is disabled on an interface by default.

1.3.8 Creating a Virtual Link

1. Overview

In the OSPF routing domain, all the areas must be connected to the backbone area. If the backbone area is disconnected, a virtual link must be configured to connect to the backbone area; otherwise, network communication problems will occur. A virtual link must be created between two ABRs, and the area to which both ABRs belong is the transit area. A stub area or an NSSA cannot be used as a transit area. A virtual link can also be used to connect other non-backbone areas.

2. Restrictions and Guidelines

- Only the authentication key of the virtual link is defined in a virtual link. To enable OSPF packet authentication in the areas connected to the virtual link, run the **area authentication** command to enable the authentication.
- The virtual link supports the fast hello function.
  - If the fast hello function is configured for a virtual link, the hello interval field of the hello packet advertised on the virtual link is set to 0, and the hello interval field of the hello packet received on this virtual link is ignored.
  - No matter whether the fast hello function is enabled, the neighbor dead interval must be always consistent on the devices at both ends of the virtual link.

- The **dead-interval**, **minimal hello-multiplier**, and **hello-interval** parameters introduced for the fast hello function cannot be configured simultaneously.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure a virtual link.

area *area-id* **virtual-link** *router-id* [**authentication** [**keychain** *kechain-name* | **message-digest** | **null**] | **dead-interval** { *dead-interval* | **minimal hello-multiplier** *multiplier-time* } | **hello-interval** *hello-interval* | **retransmit-interval** *retransmit-interval* | **transmit-delay** *transmit-delay*] * [**authentication-key** [**0** | **7**] *key* | **message-digest-key** *key-id* **md5** [**0** | **7**] *key*]

No virtual link is configured by default.

1.4 Configuring OSPF Network Type

1.4.1 Overview

If the physical network is X.25, frame relay, or ATM, set an OSPF network type so that the network can also run OSPF and provide IPv4 unicast routing service.

OSPF classifies networks into five types according to the link layer protocol type so that LSAs are exchanged in different ways to set up an adjacency. You can configure to forcibly change the network type of an interface.

1.4.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- The network types must be consistent for the devices at both ends of the link. Otherwise, the neighbor relationship cannot be set up.
- The broadcast network sends multicast OSPF packets, automatically discovers neighbors, and elects a DR and a BDR.
- The P2P network sends multicast OSPF packets and automatically discovers neighbors.
- The NBMA network sends unicast OSPF packets. Neighbors must be manually specified, and a DR and a BDR must be elected.
- The P2MP network (without carrying the **non-broadcast** parameter) sends multicast OSPF packets. Neighbors are automatically discovered.

- The P2MP network (carrying the **non-broadcast** parameter) sends unicast OSPF packets. Neighbors must be manually specified.

1.4.3 Configuration Tasks

The OSPF network type configuration includes the following tasks:

(1) Configuring the Interface Network Type

(2) (Optional) Configuring a Neighbor

(3) (Optional) Configuring the Interface Priority

(4) (Optional) Disabling Source Address Verification

1.4.4 Configuring the Interface Network Type

1. Overview

By default, Ethernet and FDDI belong to the broadcast type, X.25, frame relay, and ATM belong to the NBMA type, and PPP, HDLC, and LAPB belong to the P2P type.

2. Restrictions and Guidelines

- The configuration is required on routers at both ends of the link.
- The broadcast type requires that the interface must have the broadcast capability.
- The P2P type requires that the interfaces are interconnected in one-to-one manner.
- The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a network type for the interface.

ip ospf network { **broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point** }

By default, the network interface of OSPF is not configured, and no interface is set to P2MP type.

1.4.5 Configuring a Neighbor

1. Overview

On the NBMA network, routers cannot send or receive broadcast packets, and cannot discover neighbors through hello packets. You need to specify neighbors manually and send unicast hello packets.

If a neighbor router becomes inactive on the NBMA network, OSPF still sends hello packets to this neighbor even if no hello packet is received within the router failure time. The interval at which the hello packet is sent is called polling interval. When running for the first time, OSPF sends hello packets only to neighbors whose priorities are not 0. In this way, neighbors with priorities set to 0 do not participate in the DR/BDR election. After a DR/BDR is elected, the DR/BDR sends the hello packets to all neighbors to set up a neighbor relationship.

2. Restrictions and Guidelines

- If the network type of an interface is set to NBMA or P2MP (carrying the **non-broadcast** parameter), neighbors must be configured.
- Neighbors are configured on routers at both ends of the NBMA or P2MP (carrying the **non-broadcast** parameter) network.
- The neighbor IP address must be the primary IP address of this neighbor interface.
- The P2MP (non-broadcast) network cannot dynamically discover neighbors because it does not have the broadcast capability. Therefore, you must run this command to manually configure neighbors for the P2MP (non-broadcast) network.
- You can use the **cost** parameter to specify the cost to reach each neighbor on the P2MP network.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure a neighbor.

neighbor *ipv4-address* [**cost** *cost* | [**poll-interval** *poll-interval* | **priority** *priority*] *]

No neighbor is configured by default. Neighbors must be specified for the NBMA or P2MP (non-broadcast) interfaces. The neighbor IP address must be the primary IP address of this neighbor interface. In addition, you can use the **cost** parameter to specify the cost to reach each neighbor on the P2MP network.

1.4.6 Configuring the Interface Priority

1. Overview

When the DR/BDR election occurs on the OSPF broadcast network, the router with the highest priority becomes the DR or BDR. If the priorities are the same, the router with the largest router ID becomes the DR or BDR. A router with the priority set to 0 does not participate in the DR/BDR election. The priority value of an OSPF interface is contained in the hello packet.

2. Restrictions and Guidelines

- This command is applicable only to the OSPF broadcast and NBMA interfaces.
- You must configure the interface priority if a router must be specified as a DR, or a router cannot be specified as a DR.
- Configure the interface priority on a router that must be specified as a DR, or cannot be specified as a DR.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the interface priority.

ip ospf priority *priority*

The priority value is 1 by default.

1.4.7 Disabling Source Address Verification

1. Overview

Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information is notified during the P2P link negotiation, OSPF checks whether the source address of the packet is the address advertised by the peer end during negotiation. If not, OSPF determines that the packet is invalid and discards it. Besides, OSPF does not verify the address of an unnumbered interface.

In some scenarios, the source address of a packet received by OSPF may not be in the same network segment as the receiving interface, so the OSPF address verification fails. For example, the negotiated peer address cannot be obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

2. Restrictions and Guidelines

- The OSPF basic functions must be configured.
- Source address verification cannot be disabled on a broadcast or NBMA network.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Disable source address verification.

ip ospf source-check-ignore

The source address verification on a P2P link is enabled by default.

1.5 Adjusting OSPF Routing

1.5.1 Overview

Change the OSPF routes so that the traffic passes through specified nodes or bypasses specified nodes. Change the sequence that a router selects routes so as to change the priorities of OSPF routes.

1.5.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

1.5.3 Configuration Tasks

The configuration for adjusting OSPF routing includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring the AD
- Configuring the Reference Bandwidth
- Configuring the Cost of an Interface
- Configuring Cost Fallback Value for an AP
- Configuring the Cost of the Default Route in a Stub Area or an NSSA
- Configuring the Default Metric Value for Redistribution value
- Configuring the Maximum Metric

- Configuring RFC1583 Compatibility
- Configuring Association of External Route Forwarding Addresses with Interface Configuration

1.5.4 Configuring the AD

1. Overview

AD is used to select the best path when multiple routing protocols are used to reach the same target. AD defines the reliability of routing protocol. A smaller AD indicates higher reliability and higher routing priority. The default AD values of OSPF intra-domain routes, inter-domain routes, and external routes are all 110. Different ADs can be set to control routing.

2. Restrictions and Guidelines

- Perform this configuration if you hope to change the priorities of OSPF routes on a router that runs multiple unicast routing protocols.
- Run this command to specify different ADs for different types of OSPF routes.
- Configure the **route-map** parameter and set an AD for the specific route through a policy. If the route map is configured with **set distance**, then:
  - Through the matched route: the AD is set by the **set distance** command.
  - Not through the matched route: the AD is set by the **distance** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure an AD.

distance { *distance* [**route-map** *map-name*] | **ospf** { [**intra-area** *distance* [**route-map** *map-name*]] [**inter-area** *distance* [**route-map** *map-name*]] [**external** *distance* [**route-map** *map-name*]] } }

By default, the management distance is **110** for all the OSPF routes.

1.5.5 Configuring the Reference Bandwidth

1. Overview

The default value of OSPF reference bandwidth is 100 Mbps, and the cost is the actual bandwidth divided by the reference bandwidth. In the Gigabit and 10 Gigabit network environments, the calculated cost value is 1, so the default bandwidth value cannot adapt to the current high-speed transport network. A router is connected to lines

with different bandwidths. You are advised to adjust the configuration according to the actual bandwidth if you want to preferentially select the line with a larger bandwidth.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the reference bandwidth.

auto-cost reference-bandwidth *ref-bw*

By default, the reference bandwidth value of interface metric calculation is 100 Mbps.

1.5.6 Configuring the Cost of an Interface

1. Overview

Modifying the interface cost of OSPF can optimize routing. A lower cost of the link indicates a higher priority during routing.

2. Restrictions and Guidelines

- By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth.
- A router is connected with multiple lines. This configuration is recommended if you wish to manually specify a preferential line.
- Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps.
- Run the **bandwidth** command to set the interface bandwidth.
- The default costs of OSPF interfaces on several typical lines are as follows:
  - 64 Kbps serial line: The cost is 1562.
  - E1 line: The cost is 48.
  - 10M Ethernet: The cost is 10.
  - 100M Ethernet: The cost is 1.
- If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the cost of an interface.

ip ospf cost *cost*

By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth (the reference bandwidth is 100 Mbps by default).

1.5.7 Configuring Cost Fallback Value for an AP

1. Overview

The bandwidth of an AP is equal to the sum of the bandwidths of all the valid member ports. When a member port fails, the bandwidth of the AP will be reduced. You can set a cost fallback value for the AP to enable OSPF to select other paths preferably. When the failed member port of the AP recovers, the cost fallback value becomes invalid, and the metric of the AP returns to normal.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the cost fallback value for an AP.

ip ospf cost-fallback *cost* **threshold** *bandwidth*

The cost fallback function is disabled on an AP by default.

1.5.8 Configuring the Cost of the Default Route in a Stub Area or an NSSA

1. Overview

After an area is set to a stub area/NSSA, ABR will advertise the default route to the stub area/NSSA, ensuring that the routes from the stub area/NSSA to other areas are reachable. The default cost of a default route is 1. This function can adjust the cost of the default route and flexibly control the routes of the stub area and NSSA.

2. Restrictions and Guidelines

This command takes effect only on an ABR in a stub area or on an ABR/ASBR in an NSSA.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the cost of the default route in a stub area or an NSSA.

area *area-id* **default-cost** *cost*

By default, the cost of a route is 1.

1.5.9 Configuring the Default Metric Value for Redistribution

1. Overview

When redistributing external routes, you can configure the costs of external routes to adjust routing flexibly.

2. Restrictions and Guidelines

- This configuration is mandatory if the cost of external routes of the OSPF domain should be specified when external routes are introduced to an ASBR.
- The **default-metric** command must be used together with the **redistribute** command in routing process configuration mode to modify the initial metrics of all redistributed routes.
- The **default-metric** command does not take effect on external routes that are injected to the OSPF routing domain using the **default-information originate** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the default metric for redistribution.

default-metric *metric*

By default, the metric of a redistributed route is 20.

1.5.10 Configuring the Maximum Metric

1. Overview

In the scenarios of restarting a device and using a device as a candidate path, the OSPF information advertised by the current device can be configured with the maximum metric value so that the data traffic will not pass through the current device.

2. Restrictions and Guidelines

- A router may be unstable in the restart process or a period of time after the router is restarted, and users do not want to forward data traffic through this router. In this case, this configuration is recommended.
- After the **max-metric router-lsa** command is configured, the metrics of the non-stub links in the router LSAs generated by the router will be set to the maximum value (0xFFFF). If you cancel this configuration or the timer expires, the normal metrics of the links are restored.
- By default, if the **max-metric router-lsa** command is configured, the stub links still advertise common metrics, that is, the costs of outbound interfaces. If the **include-stub** parameter is configured, the stub links will advertise the maximum metric.
- If an ABR is not intended to transfer inter-area traffic, use the **summary-lsa** parameter to set the metric of the summary LSA to the maximum value.
- If an ASBR does not wish to transfer external traffic, use the **external-lsa** parameter to set the metric of the external LSA to the maximum value.
- The **max-metric router-lsa** command is generally used in the following scenarios:
  - Restart a device. After the device is restarted, IGP generally converges faster, and other devices attempt to forward traffic through the restarted device. If the current device is still building the BGP routing table and some BGP routes are not learned yet, packets sent to these networks are discarded. In this case, you can use the **on-startup** parameter to set a delay after which the restarted device acts as the transmission mode.
  - Add a device to the network but the device is not used to transfer traffic. The device is added to the network. If a candidate path exists, the current device is not used to transfer traffic. If a candidate path does not exist, the current device is still used to transfer traffic.
  - Delete a device gracefully from the network. After the **max-metric router-lsa** command is configured, the current device advertises the maximum metric among all the routes. In this way, other devices on the network can select the backup path for data transmission before the device is shut down.
  - In the earlier OSPF version (RFC1247 or earlier), the links with the maximum metric (0xFFFF) in the LSAs do not participate in the SPF computation, that is, no traffic is sent to routers that generate these LSAs.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the maximum metric.

max-metric router-lsa [**external-lsa** [*max-metric-value*] | **include-stub** | **on-neighborup** [*full-interval-time*] | **on-startup** [*startup-interval-time*] | **summary-lsa** [*max-metric-value*]] *

By default, the LSAs of normal metric are advertised.

1.5.11 Configuring RFC1583 Compatibility

1. Overview

When there are multiple paths to an ASBR or the forwarding address of an external route, RFC1583 and RFC2328 define different routing rules. If RFC1583 compatibility is configured, a path in the backbone area or an inter-area path is preferentially selected. If RFC1583 compatibility is not configured, a path in a non-backbone area is preferentially selected.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure compatible RFC1583.

compatible rfc1583

The RFC1583 rule function is enabled by default.

1.5.12 Configuring Association of External Route Forwarding Addresses with Interface Configuration

1. Overview

Setting the forwarding address (FA) of relevant flag bit can associate the interface configuration with the external route forwarding address to calculate the reachability and metric.

2. Restrictions and Guidelines

- In the case of interconnection with a Cisco device, the FA configuration compatible with the Cisco device must

be enabled.

- When the FA of an external route is 0, external route computation of OSPF will compute the reachability and metric to the advertiser. When the FA is not 0, the reachability and metric to the forwarding address will be computed.
- When the following conditions are met simultaneously in default configuration, the ASBR of OSPF fills the forwarding address field of the external route with digits other than 0:
  - OSPF is enabled on the next hop interface for connecting the ASBR to external network.
  - The next hop interface for connecting the ASBR to the external network is in the network scope advertised in the OSPF protocol.
- When the following conditions are met simultaneously after association of forwarding address rules with interface configuration is configured, the ASBR of OSPF fills the forwarding address field of the external route with digits other than 0:
  - OSPF is enabled on the next hop interface for connecting the ASBR to external network.
  - The next hop interface for connecting the ASBR to the external network is in the network scope advertised in the OSPF protocol.
  - The next hop interface for connecting the ASBR to the external network is not configured as a passive interface.
  - The next hop interface for connecting the ASBR to the external network is not P2P or P2MP type of OSPF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

1.6 Configuring OSPF Route Advertisement

1.6.1 Overview

The function aims to introduce unicast routes for other AS domains or default routes to other AS domains to the OSPF domain and provide the unicast routing service to other AS domains for users in the OSPF domain. The router that introduces routes will automatically become an ASBR.

OSPF has two types of external routes. The metric of the Type-1 external route changes, but the metric of the Type-2 external route is fixed. If two parallel paths to the same destination network have the same route metric, the

priority of Type-1 route is higher than that of Type-2 route. Therefore, the **show ip route** command displays only the Type-1 route.

1.6.2 Restrictions and Guidelines

The OSPF basic functions must be configured.

1.6.3 Configuration Tasks

The configuration of OSPF route advertisement includes the following tasks:

(1) Configuring External Route Redistribution

(2) Generating a Default Route

(3) (Optional) Configuring a Device as ASBR

1.6.4 Configuring External Route Redistribution

1. Overview

Configure external route redistribution if external routes of the OSPF domain need to be introduced to an ASBR.

2. Restrictions and Guidelines

- Perform this configuration on an ASBR.
- After this command is configured, the router becomes an ASBR, imports related routing information to the OSPF domain, and advertises the routing information as Type-5 LSAs to other OSPF routers in the domain.
- If the **level** parameter is not carried when IS-IS route redistribution is configured, only Level-2 routes can be redistributed by default. The **level** parameter is carried during initial configuration of redistribution, the routes configured with the **level** parameter can be redistributed. If both **level 1** and **level 2** are configured, the two levels are combined and saved as **level-1-2**.
- If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be distributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can run the **no** form of the command to restore the default value of **match**.
- If **route-map** is specified, the **match** filtering rules specified in **route-map** are applicable to the original parameters of redistribution. For redistribution of OSPF or IS-IS routes, **route-map** is used for filtering only when the redistributed routes meet the criteria specified by **match** or **level**.
- The **set metric** value range of the associated **route-map** is from 0 to 16777214. If the value exceeds this range, routes cannot be introduced.
- The configuration rules for the **no** form of the **redistribute** command are as follows:
  - If some parameters are specified in the **no** form of this command, default values of these parameters will be restored.
  - If no parameter is specified in the **no** form of this command, the entire command will be deleted.

- For example, if **redistribute isis 112 level-2** is configured, you can run the **no redistribute isis 112 level-2** command to restore the default value of level-2. As **level-2** itself is the default value of the parameter, the configuration saved is still **redistribute isis 112 level-2** after the preceding **no** form of the command is executed. To delete the entire command, run the **no redistribute isis 112** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure external route redistribution.

redistribute { **arp-host** | **bgp** | **connected** | **isis** [*area-tag*] [**level-1** | **level-1-2** | **level-2**] | **ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **rip** | **static** } [**metric** *metric-value* | **metric-type** { **1** | **2** } | **route-map** *route-map-name* | **subnets** | **tag** *tag-value*] *

The route redistribution function is not configured by default.

1.6.5 Generating a Default Route

1. Overview

A default route needs to be introduced to an ASBR so that other routers in the OSPF domain access other AS domains through this ASBR by default.

2. Restrictions and Guidelines

- When the **redistribute** or **default-information** command is executed, the OSPF router automatically becomes an ASBR. The ASBR, however, does not automatically generate or advertise a default route to all routers in the OSPF routing domain. To enable an ASBR to generate a default route, configure the **default-information originate** command.
- The metric of the external default route can only be defined in the **default-information originate** command, instead of the **default-metric** command.
- A router in a stub area cannot generate an external default route.
- The **set metric** value range of the associated **route-map** is from 0 to 16777214. If the value exceeds this range, routes cannot be introduced.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Generate a default route.

default-information originate [**always** | **metric** *metric* | **metric-type** *type* | **route-map** *map-name*] *

No default route is generated by default.

If the **always** parameter is specified, the OSPF routing process advertises an external default route to neighbors regardless of whether a default route exists. This default route, however, is not displayed on the local router. To confirm whether the default route is generated, run the **show ip ospf database** command to display the OSPF LSDB. The external link with the ID 0.0.0.0 describes the default route. On an OSPF neighbor, you can run the **show ip route** command to see the default route.

1.6.6 Configuring a Device as ASBR

1. Overview

Configure a device as ASBR in the AS domain or AS boundary.

2. Restrictions and Guidelines

After the **redistribute** or **default-information** command is executed, the OSPF router automatically becomes an ASBR. If you want the device to become an ASBR without configuring the above command, configure the **asbr enable** command. If the **asbr enable** command is deleted, but the **redistribute** or **default-information** command is still configured, the device is still an ASBR.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure a device as ASBR.

asbr enable

ASBR is disabled by default.

1.7 Configuring OSPF Route Summarization

1.7.1 Overview

Summarize routes to reduce interaction of routing information and the size of routing table, and enhance stability of routes. Shield or filter routes.

1.7.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- The address range of the route to be summarized may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table to shield or filter routes.

1.7.3 Configuration Tasks

The configuration of OSPF route summarization includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring Inter-Area Route Summarization
- Configuring External Route Summarization
- Configuring a Discard Route

1.7.4 Configuring Inter-Area Route Summarization

1. Overview

On a large-scale OSPF network, configuring route summarization can reduce the size of a routing table and the LSA information, thus reducing the system loss.

2. Restrictions and Guidelines

- Perform this configuration when routes of the OSPF area need to be summarized.
- Unless otherwise required, perform this configuration on an ABR in the area where routes to be summarized are located.
- This command can be executed only on the ABR. It is used to combine or summarize multiple routes of an area into one route, and then advertise the route to other areas. Combination of the routing information occurs only on the boundary of an area. Routers inside the area can learn specific routing information, whereas routers in other areas can learn only one summarized route. You can set **advertise** or **not-advertise** to determine whether to advertise this summarized route to shield and filter routes. By default, the summarized route is advertised. You can use the **cost** parameter to set the metric of the summarized route.
- You can configure the route summarization command for multiple areas. This simplifies routes in the entire OSPF routing domain, and improves the network forwarding performance, especially for a large-sized network.

- When multiple routes for summarization are configured and have an inclusive relationship with each other, the range of routes to be summarized is determined based on the longest match principle.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure inter-area route summarization.

area *area-id* **range** *ipv4-address mask* [**advertise** | **not-advertise**] [**cost** *cost* | **inherit-minimum**]

The inter-area route summarization function is disabled by default.

1.7.5 Configuring External Route Summarization

1. Overview

When a lot of OSPF domain routes need to be introduced, configuring route summarization can reduce the size of a routing table and the LSA information, thus reducing the system loss.

2. Restrictions and Guidelines

- Perform this configuration when routes outside the OSPF domain need to be summarized.
- Unless otherwise required, perform this configuration on an ASBR, to which routes that need to be summarized are introduced.
- When routes are redistributed from other routing processes and injected to the OSPF routing process, every route is advertised to the OSPF routers using an external LSA respectively. If the injected routes are in a continuous address space, the ASBR can advertise only one summarized route to significantly reduce the size of the routing table.
- The **area range** command summarizes the routes between OSPF areas, whereas **summary-address** summarizes external routes of the OSPF routing domain.
- When configured on the NSSA ABR translator, **summary-address** summarizes redistributed routes and routes obtained based on the LSAs that are converted from Type 7 to Type 5. When configured on the ASBR (not an NSSA ABR translator), **summary-address** summarizes only redistributed routes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure external route summarization.

summary-address *ipv4-address mask* [[**cost** *cost* | **distribute-delay** *interval* | **nssa-only** | **tag** *tag-value*] * | **not-advertise**]

The route summarization function is disabled by default.

1.7.6 Configuring a Discard Route

1. Overview

The address range of summarized routes may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table on the ABR or ASBR. This route is automatically generated, and is not advertised.

The discard route means adding a route whose egress is Null 0 to the routing table, and it will not generate the corresponding LSA, so it will not be received by neighbors. The packets matching the route are discarded.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure a discard route.

discard-route { **internal** | **external** }

The discard route adding function is enabled by default.

1.8 Configuring OSPF Route Filtering

1.8.1 Overview

Routes that do not meet filtering conditions cannot be loaded to the routing table, or advertised to neighbors. Network users cannot access specified destination network.

1.8.2 Restrictions and Guidelines

The OSPF basic functions must be configured.

1.8.3 Configuration Tasks

The configuration of OSPF route filtering includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring a Passive Interface
- Configuring LSA Update Packet Filtering
- Configuring Inter-area Route Filtering
- Configuring Redistributed Route Filtering
- Configuring Learned Route Filtering

1.8.4 Configuring a Passive Interface

1. Overview

To prevent other routers on the network from learning the routing information of the local router, you can configure a specified network interface of the local router as the passive interface, or a specified IP address of a network interface as the passive address.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure a passive interface.

passive-interface { **default** | *interface-type interface-number* | *interface-type interface-number ipv4-address* }

By default, the passive modes of all interfaces are disabled, and all interfaces are allowed to send and receive OSPF packets.

1.8.5 Configuring LSA Update Packet Filtering

1. Overview

Enable this function on an interface to prevent sending the LSA update packet from this interface. After this function is enabled, the local router does not advertise the LSA update packet to neighbors, but still sets up an adjacency with neighbors and receives LSAs from neighbors.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure LSA update packet filtering.

ip ospf database-filter all out

By default, the function of not diffusing LSA packets to the outside is disabled on an interface, that is, any LSA update packet can be sent from the interface.

1.8.6 Configuring Inter-area Route Filtering

1. Overview

Route filtering can prevent routes from being loaded to the routing table or advertised to neighbors. Network users cannot access the specified destination network.

Routers are filtered using the following three methods.

- When an interface is configured as a passive interface, it no longer sends or receives hello packets.
- Configure **distribute-list out** if external routes introduced by the ASBR need to be filtered.
- To prevent users from accessing the specified destination network, configure **distribute-list in** to filter the routes that are computed based on the received LSA. Only the routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors.

2. Restrictions and Guidelines

- This command can be configured only on an ABR.
- Run this command when it is required to configure filtering conditions for inter-area routes on the ABR.
- This configuration is recommended if users need to be prevented from accessing the network in a certain OSPF area.
- Unless otherwise required, perform this configuration on an ABR in the area where filtered routes are located.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ACL or prefix list. Please configure only one task.

- Configure an ACL.

  access-list *acl-number* { **deny** | **permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *tm-range-name*] [**log**]

- Configure a prefix list.

  ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

(4) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(5) Configure inter-area route filtering.

area *area-id* **filter-list** { **access** *acl-number* | **prefix** *prefix-list-name* } { **in** | **out** }

By default, the filtering list function is not configured on an ABR.

1.8.7 Configuring Redistributed Route Filtering

1. Overview

Similar to the **redistribute route-map** command, the **distribute-list out** command is used to filter routes that are redistributed from other protocols to OSPF. The command itself does not redistribute routes, and is generally used together with the **redistribute** command.

2. Restrictions and Guidelines

- Perform this configuration if external routes introduced by the ASBR need to be filtered.
- Unless otherwise required, perform this configuration on an ASBR to which filtered routes are introduced.
- The ACL and prefix list filtering rules are mutually exclusive in the configuration. In other words, if the ACL is used for filtering routes coming from a certain a source, the prefix list cannot be configured to filter the same routes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ACL or prefix list. Please configure only one task.

- Configure an ACL.

  access-list *acl-number* { **deny** | **permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *tm-range-name*] [**log**]

- Configure a prefix list.

ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

(4) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(5) Configure redistributed route filtering.

distribute-list { *acl-number* | *acl-name* | **prefix** *prefix-list-name* } **out** [**arp-host** | **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

By default, the filtering function of redistributed routes is disabled, that is, all the redistributed routes get past.

1.8.8 Configuring Learned Route Filtering

1. Overview

This function filters the routes that are computed based on received LSAs. Only the routes meeting the filtering conditions can be forwarded.

2. Restrictions and Guidelines

Filtering routes by using the **distribute-list in** command affects forwarding of local routes only, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type-3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black hole routes are generated. In this case, you can run the **area filter-list** or **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black hole routes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ACL or prefix list. Please configure only one task.

- Configure an ACL.

  istribute-list { *acl-name* | *acl-number* | **gateway** *prefix-list-name* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* } **in** [*interface-type interface-number*]

- Configure a prefix list.

  ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

(4) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(5) Configure learned route filtering.

distribute-list { [*acl-number* | *acl-name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

By default, the filtering function of the routes calculated based on the received LSA is disabled, that is, all these routes get past.

1.9 Adjusting OSPF Network Convergence Speed

1.9.1 Overview

This function aims to modify protocol control parameters to change the protocol running status, thus adjusting the convergence speed of OSPF network.

1.9.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- The neighbor relationship maintenance time cannot be shorter than the hello interval.

1.9.3 Configuration Tasks

The configuration for adjusting the convergence speed of OSPF network includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring the Hello Interval
- Configuring the Dead Interval
- Configuring LSU Transmission Delay
- Configuring LSU Retransmission Interval
- Configuring LSU Generation Time
- Configuring LSA Group Refresh Time
- Configuring LSA Group Refresh Interval
- Configuring Duplicate LSA Receiving Delay
- Configuring Inter-Area Route Computation Delay
- Configuring External Route Computation Delay
- Configuring SPF Computation Delay
- Enabling Two-Way Maintenance

1.9.4 Configuring the Hello Interval

1. Overview

The hello packet interval is contained in the hello packet. A shorter hello interval indicates that OSPF can detect topology changes more quickly, but the network traffic increases.

2. Restrictions and Guidelines

- This configuration is performed on routers at both ends of a link.
- The hello packet interval must be the same on all routers in the same network segment. If you want to manually modify the neighbor dead interval, ensure that the neighbor dead interval is longer than the hello packet interval.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the hello interval.

ip ospf hello-interval *hello-interval*

By default, the hello packet interval is 10s for Ethernet, PPP, HDLC encapsulation interfaces, and frame relay point-to-point sub-interfaces; the hello packet interval is 30s for non-frame relay point-to-point sub-interfaces and X.25 interfaces.

1.9.5 Configuring the Dead Interval

1. Overview

This configuration can be adjusted if you wish to accelerate OSPF convergence when a link fails. The failure determining interval of an OSPF neighbor is contained in the hello packet. If OSPF does not receive a hello packet from a neighbor within the neighbor dead interval, it declares that the neighbor is invalid and deletes this neighbor record from the neighbor list.

2. Restrictions and Guidelines

- This configuration is performed on routers at both ends of a link.
- By default, the dead interval is four times the hello packet interval. If the hello packet interval is modified, the dead interval is modified automatically.
- Be sure to run this command to manually modify the interval for OSPF to judge failure of a neighbor with caution. Pay attention to the following two issues:
  - The neighbor dead interval cannot be smaller than the hello packet sending interval;
  - The neighbor dead interval must be the same on all routers in the same network segment.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the **dead** interval.

ip ospf dead-interval { *dead-interval* | **minimal hello-multiplier** *multiplier* }

By default, the fast hello function is disabled, and the neighbor dead interval is four times the sending interval of hello packet.

1.9.6 Configuring LSU Transmission Delay

1. Overview

On a low speed network, a device can be configured with the delay before sending LSU packets.

2. Restrictions and Guidelines

- Before an LSU packet is transmitted, the **Age** fields in all LSAs in this packet will increase based on the amount specified by the LSU transmission delay. Considering the transmission delay and line propagation delay on the interface, you need to set the LSU transmission delay to a greater value for a low-speed line or interface. The LSU packet transmission delay of a virtual link is defined by the **transmit-delay** parameter in the **area virtual-link** command.
- If the value of the **Age** field of an LSA reaches 3600, the packet will be retransmitted or a retransmission request will be sent. If the LSA is not updated in time, the expired LSA will be deleted from the LSDB.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the LSU transmission delay.

ip ospf transmit-delay *transmit-delay*

The LSU packet transmission delay is 1s by default.

1.9.7 Configuring LSU Retransmission Interval

1. Overview

When a network is congested, frequent LSU retransmission will aggravate the congestion. The retransmission delay can be set to a greater value on a serial line or virtual link to prevent unwanted retransmission. The LSU retransmission interval of a virtual link is defined by the **retransmit-interval** parameter in the **area virtual-link** command.

After a router finishes sending an LSU packet, this packet is still kept in the transmit buffer queue. If an acknowledgment from the neighbor is not received within the LSU retransmission interval, the router retransmits the LSU packet.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the LSU retransmission interval.

ip ospf retransmit-interval *retransmit-interval*

By default, the LSU retransmission interval is 5s.

1.9.8 Configuring LSU Generation Time

1. Overview

The LSU generation time can be adjusted according to different requirements for network performance and convergence speed.

2. Restrictions and Guidelines

- If a high convergence requirement is raised when a link changes, you can set *delay-time* to a smaller value. You can also appropriately increase the values of the preceding parameters to reduce the CPU usage.
- When configuring this command, the value of *hold-time* cannot be smaller than the value of *delay-time*, and the value of *max-wait-time* cannot be smaller than the value of *hold-time*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the exponential backoff algorithm for generating LSAs.

timers throttle lsa all *delay-time hold-time max-wait-time*

By default, the minimum delay of LSA generation is 0 ms, the minimum interval between the first update and the second update of LSA is 5000 ms, and the maximum interval between consecutive LSA updates is 5000 ms.

1.9.9 Configuring LSA Group Refresh Time

1. Overview

Every LSA has its time to live (LSA age). When the LSA age reaches 3600s, a refreshment is needed to prevent normal LSAs from being cleared because their ages reaching the maximum. If LSA update and aging computation are performed for every LSA, the device will consume a lot of CPU resources. To use CPU resources effectively, you can refresh LSAs by group on the device. Allocate the LSAs received within a certain time (pacing interval) to the same group. The device will maintain a refresh timer for this group. After the timer expires, the LSAs in the group will be refreshed uniformly.

2. Restrictions and Guidelines

If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout, which will lead to a high load of the CPU in a certain period of time. For CPU stability, the number of LSAs processed upon each timeout cannot be too large. If the number of LSAs is large, you are advised to reduce the group pacing interval. For example, if there are 10,000 LSAs in the database, you can reduce the pacing interval; if there are 40 to 100 LSAs, you can set the pacing interval to 10-20 minutes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the LSA group refresh time.

timers pacing lsa-group *pacing-interval*

The group pacing interval of LSA is 30s by default.

1.9.10 Configuring LSA Group Refresh Interval

1. Overview

If a router has a large number of routing entries, synchronizing LSDB will send a large number of LSU packets, easily causing network congestion. The LSU packets can be grouped and sent at an interval to ensure stability of the network.

2. Restrictions and Guidelines

- If the number of LSAs is large and the device load is heavy in an environment, properly configuring *transimit-time* and *transimit-count* can limit the number of LS-UPD packets flooded on the network.
- If the CPU usage is not high and the network bandwidth load is not heavy, reducing the value of *transimit-time* and increasing the value of *transimit-count* can accelerate the environment convergence.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the LSA group refresh interval.

timers pacing lsa-transmit *transmit-interval transmit-count*

By default, the interval for sending LSU group is 40 ms, and the number of LS-UPD packets in each group is 1.

1.9.11 Configuring Duplicate LSA Receiving Delay

1. Overview

According to the network connection and equipment resources of the current network, you can configure that no processing is performed if the same LSA is received within the specified time. This prevents excessive usage of network bandwidth and equipment resources caused by network connection or frequent route flapping.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure duplicate LSA receiving delay.

timers lsa arrival *arrival-time*

By default, the delay for receiving a duplicate LSA is 1000 ms.

1.9.12 Configuring Inter-Area Route Computation Delay

1. Overview

In case of route flapping, frequent inter-area route computation will consume a lot of device performance, and delaying the process of inter-area route computation can reduce the device load.

2. Restrictions and Guidelines

- This delay cannot be modified if strict requirements are raised for the network convergence time.
- If a lot of inter-area or external routes exist on the network and the network is not stable, you can adjust the corresponding delays.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure inter-area route computation delay.

timers throttle route inter-area *ia-delay*

By default, the waiting time for inter-area route computation is 0 ms.

1.9.13 Configuring External Route Computation Delay

1. Overview

In case of route flapping, frequent external route computation will consume a lot of device performance, and delaying the process of external route computation can reduce the device load.

2. Restrictions and Guidelines

- This delay cannot be modified if strict requirements are raised for the network convergence time.
- If a lot of inter-area or external routes exist on the network and the network is not stable, you can adjust the corresponding delays.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the external route computation delay.

timers throttle route ase *ase-delay*

By default, the waiting time for external route computation is 0 ms.

1.9.14 Configuring SPF Computation Delay

1. Overview

Changes to LSDB will trigger SPF computation. Frequent network jitter will consume a lot of CPU resources. Setting a reasonable delay for SPF computation can avoid occupying excessive router memory and bandwidth resources.

2. Restrictions and Guidelines

- Compared with the **timers spf** command, this command supports more flexible settings to accelerate the convergence speed of SPF computation and further reduce the system resources consumed by SPF computation when the topology continuously changes. Therefore, you are advised to run the **timers throttle spf** command to adjust the SPF computation time.
- The value of *spf-holdtime* cannot be smaller than that of *spf-delay*; otherwise, *spf-holdtime* will be automatically set to the value of *spf-delay*.
- The value of *spf-max-waittime* cannot be smaller than that of *spf-holdtime*; otherwise, *spf-max-waittime* will be automatically set to the value of *spf-holdtime*.
- The configurations of **timers throttle spf** and **timers spf** are mutually overwritten.
- When neither **timers spf** nor **timers throttle spf** is configured, the default value of **timers throttle spf** prevails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the SPF computation delay.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

By default, the delay for SPF computation is 1000 ms, the minimum interval for two SPF computations is 5000 ms, and the maximum interval between two SPF computations is 10000 ms.

1.9.15 Enabling Two-Way Maintenance

1. Overview

On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the time required for processing hello packets exceeds the neighbor dead interval, the corresponding adjacency times out and is removed. If the two-way maintenance function is enabled, in addition to the hello packets, the DD, LSU, LSR, and LSAck packets from a neighbor can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist on the network. This prevents termination of the adjacency caused by delayed or discarded hello packets. The function is enabled by default. You are advised to retain the default configuration.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Enable two-way maintenance.

two-way-maintain

By default, the two-way maintenance function is enabled for an OSPF process.

1.10 Configuring Stub Area and NSSA

1.10.1 Overview

The function is used to configure an area located on the stub as a stub area to reduce interaction of routing information and the size of routing table, and enhance stability of routes.

1.10.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- A backbone or transit area cannot be configured as a stub or an NSSA area.
- A router in the stub area cannot introduce external routes, but a router in the NSSA area can introduce external routes.

1.10.3 Configuration Tasks

The configuration of stub area and NSSA includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring a Stub Area
- Configuring an NSSA

1.10.4 Configuring a Stub Area

1. Overview

The stub area is an OSPF stubby area. Configuring a stub area can reduce the number of LSAs in the stub area. The ABR in the stub area will not transfer the Type-5 LSA (external route), and the default route will be advertised to the stub area.

A totally stub area is upgraded from a stub area. The router in the totally stub area will not transfer Type-3 LSA (inter-domain route) and Type-5 LSA (external route), and the default route will be advertised to the stub area.

2. Restrictions and Guidelines

- To configure a totally stub area, add the **no-summary** keyword when running the **area stub** command on the ABR. A router in the totally stub area can learn only the internal routes of the local area, including the internal default route generated by an ABR.
- Perform this configuration if you want to reduce the size of the routing table on routers in the area.
- The area must be configured as a stub area on all routers in this area.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure a stub area.

area *area-id* **stub** [**no-summary**]

The stub area function is disabled by default.

1.10.5 Configuring an NSSA

1. Overview

An NSSA is similar to a stub area, but allows ASBR. The route redistributed by ASBR will be transferred in the NSSA in the form of Type-7 LSA, and the Type-7 LSA will be converted into Type-5 LSA on ABR and then transferred to other areas. This ABR is also called a translator. The ABR also advertises the default route to the NSSA.

2. Restrictions and Guidelines

- The **default-information-originate** parameter is used to generate a default Type-7 LSA. This parameter has different functions on the ABR and the ASBR in an NSSA. On the ABR, a Type-7 LSA default route is generated regardless of whether the default route exists in the routing table. On the ASBR (not an ABR), a Type-7 LSA default route is generated only when the default route exists in the routing table.
- Configuring a totally NSSA can further reduce the number of LSAs sent to the NSSA. You can configure the **no-summary** parameter on the ABR to prevent the ABR from sending the summary LSAs (Type-3 LSAs) to the NSSA.
- In the same NSSA, it is recommended that only one ABR serve as a translator.
- Perform this configuration if you want to reduce the size of the routing table on routers in the area and the number of LSAs in the area, and also introduce external routes of the OSPF domain to this area.
- The area must be configured as an NSSA on all routers in this area.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configuring an NSSA Area

area *area-id* **nssa** [**default-information-originate** [**metric** *metric* | **metric-type** *metric-type*] * | **no-redistribution** | **no-summary** | **translator** [**always** | **stability-interval** ***stability-interval***] *] *

The NSSA function is disabled by default.

1.11 Configuring OSPF Authentication

1.11.1 Overview

Authentication prevents routers that illegally access the network and hosts that forge OSPF packet from participating in the OSPF process. All routers connected to the OSPF network must be authenticated to ensure stability of OSPF and protect OSPF against intrusions.

1.11.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- If authentication is configured for an area, the configuration takes effect on all interfaces that belong to this area.
- If authentication is configured for both an interface and the area to which the interface belongs, the configuration for the interface takes effect preferentially.

1.11.3 Configuration Tasks

The OSPF authentication configuration includes the following tasks:

- Configuring the Authentication Type of an Area
- Configuring the Authentication Type of an Interface
- (Optional) Configuring a Plain Text Authentication Key for an Interface
- (Optional) Configuring an MD5 Authentication Key for an Interface

1.11.4 Configuring the Authentication Type of an Area

1. Overview

OSPF area authentication can improve the security of an OSPF area. The consistency in the authentication type and password is a requisite for establishing a neighbor relationship.

2. Restrictions and Guidelines

- This configuration is recommended if the same authentication type should be enabled on all the interfaces in the same area.
- Perform this configuration if a router accesses a network that requires authentication.
- The device supports three authentication types:
  - Type 0: No authentication is required. When the OSPF authentication command is not run to enable OSPF authentication, the authentication type carried in OSPF data packets is type 0.
  - Type 1: The authentication type is plain text authentication if this command is configured but does not contain the **message-digest** parameter.
  - Type 2: The authentication type is MD5 authentication if this command is configured and contains the **message-digest** parameter.

- All routers in the same OSPF area must use the same authentication type. If authentication is enabled, the authentication key must be configured on interfaces that are connected to neighbors.
- If keychain authentication is configured, the key and authentication type configured for keychain are used. Currently, keychain supports plain text authentication, Message-Digest 5 (MD5) authentication, and SM3 authentication.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the authentication type of an area.

area *area-id* **authentication** [**message-digest** | **keychain** *name*]

The OSPF area authentication function is disabled by default.

1.11.5 Configuring the Authentication Type of an Interface

1. Overview

OSPF interface authentication can improve the communication security of neighbors. The consistency in the authentication type and password is a requisite for establishing a neighbor relationship.

2. Restrictions and Guidelines

- This configuration is mandatory if different authentication types should be used on different interfaces in the same area.
- Perform this configuration if a router accesses a network that requires authentication.
- If the **ip ospf authentication** command does not contain any option, plain text authentication is enabled. If you run the **no** form of the command to restore the default authentication mode, whether authentication is enabled is determined by the authentication type that is configured in the area to which the interface belongs. If the authentication type is set to **null**, authentication is disabled forcibly. When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially.
- If keychain authentication is configured, the key and authentication type configured for keychain are used. Currently, keychain supports plain text authentication, MD5 authentication, and SM3 authentication.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the authentication type of an interface.

ip ospf authentication [**message-digest** | **null** | **keychain** *kc-name*]

By default, no authentication mode is set on an interface. In this case, the authentication type of the related area is used on the interface.

1.11.6 Configuring a Plain Text Authentication Key for an Interface

1. Overview

This configuration is required when a router accesses a network that requires plain text authentication. The key information will be inserted to the headers of all OSPF packets. If the keys are inconsistent, two directly connected devices cannot set up an OSPF neighbor relationship and cannot exchange routing information.

2. Restrictions and Guidelines

- Different keys can be configured for different interfaces, but all the routers connected to the same physical network segment must be configured with the same key.
- You must set the authentication type to plain text authentication on the related interface or in the area in advance.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure plain text authentication for an interface.

ip ospf authentication

(5) Configure a plain text authentication key for an interface.

ip ospf authentication-key [**0** | **7**] *key*

The authentication key is disabled by default.

1.11.7 Configuring an MD5 Authentication Key for an Interface

1. Overview

The MD5 cipher text authentication mode can be used to enhance security to a certain extent.

2. Restrictions and Guidelines

- MD5 authentication features high security, and therefore is recommended. You must configure either plain text authentication or MD5 authentication. The HMAC-SHA256 algorithm features the highest security and consumes the maximum performance, while the MD5 algorithm features the lowest security and consumes the minimum performance. Select one according to the actual situation.
- This configuration is required if a router accesses a network that requires MD5 authentication.
- You must set the authentication type to cipher text authentication on the related interface or in the area in advance.
- Authentication succeeds only when both *key-id* and key are matched.
- Multiple *key-id* values are configured for the same interface, and the last *key-id* configured takes effect when packets are sent, but all *key-id* values can participate in the authentication when packets are received.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure cipher text authentication for an interface.

ip ospf authentication message-digest

(5) Configure an MD5 authentication key for an interface.

ip ospf message-digest-key *key-id* **md5** [**0** | **7**] *key*

The cipher text key function is disabled by default.

1.12 Enabling Fast Reroute

1.12.1 Overview

Once OSPF detects a route failure, the router can immediately switch to the second-best route. This configuration helps shorten the traffic interruption time.

1.12.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- The LAF configuration for fast reroute is mutually exclusive with the virtual link configuration.
- The **carrier-delay** value must be set to **0** for an interface.

1.12.3 Configuration Tasks

The configuration for enabling fast reroute includes the following tasks:

- Configuring Fast Reroute
- (Optional) Configuring Interface LFA Protection
- (Optional) Preventing an Interface From Becoming a Backup Interface

1.12.4 Configuring Fast Reroute

1. Overview

This configuration is required if you want to increase the OSPF network convergence speed to the millisecond level.

2. Restrictions and Guidelines

- This configuration is performed on a router that has multiple paths to a destination network.
- It is recommended that automatic computation of loop-free alternate (LFA) for the backup path be disabled if any of the following cases exists on the network:
  - Virtual links exist.
  - Alternative ABRs exist.
  - An ASBR is also an ABR.
  - Multiple ABSRs advertise the same external route.
- When the OSPF fast reroute function is used, it is recommended that BFD be enabled at the same time so that the device can quickly detect any link failure and therefore shorten the forwarding interruption time. If the interface is Up or Down, to shorten the forwarding interruption time during OSPF fast reroute, you can configure **carrier-delay 0** in Layer-3 interface configuration mode to achieve the fastest switchover speed.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure fast reroute.

fast-reroute { **lfa** [**downstream-paths**] | **route-map** *route-map-name* }

The fast reroute function is disabled by default.

1.12.5 Configuring Interface LFA Protection

1. Overview

A backup route is generated for the primary route based on the LFA protection mode specified in interface configuration mode. By default, LFA protection is enabled on each OSPF interface, and a failure of the primary link does not affect data forwarding on the backup route.

2. Restrictions and Guidelines

This command does not take effect if **fast-rerotue route-map** is configured.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure interface LFA protection.

ip ospf fast-reroute protection { **node | link-node | disable** }

The LFA link protection function is enabled by default.

1.12.6 Preventing an Interface From Becoming a Backup Interface

1. Overview

This configuration is mandatory if you hope that data traffic is not switched over to a specified path after the best path fails. After the best path fails, the traffic will be switched over to another second-best path, but a new best path will be selected based on the interface costs after OSPF converges again.

2. Restrictions and Guidelines

- If the remaining bandwidth of an interface is small or if the interface and its primary interface may fail at the same time, the interface cannot be used as a backup interface. Therefore, you need to run this command in interface configuration mode to prevent this interface from becoming a backup interface during OSPF fast reroute computation. After this command is executed, a backup interface will be selected from the other interfaces.
- This command does not take effect if **fast-rerotue route-map** is configured.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Prevent an interface from becoming a backup interface.

ip ospf fast-reroute no-eligible-backup

By default, an interface can be used as a backup interface of OSPF fast reroute.

1.13 Modifying the Maximum Number of Concurrent Neighbors

1.13.1 Overview

This function can control the maximum number of concurrent neighbors on the OSPF process to ease the pressure on the device.

1.13.2 Restrictions and Guidelines

The OSPF basic functions must be configured.

1.13.3 Configuration Tasks

The configuration of modifying the maximum number of concurrent neighbors includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring the Maximum Number of Concurrent Neighbors on the Current Process
- Configuring the Maximum Number of Concurrent Neighbors on All Processes

1.13.4 Configuring the Maximum Number of Concurrent Neighbors on the Current Process

1. Overview

When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which each OSPF process can concurrently initiate or accept interaction.

2. Restrictions and Guidelines

This configuration is recommended if you want to set up an OSPF adjacency more quickly when a router is connected to a lot of other routers.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the maximum number of concurrent neighbors on the current process.

max-concurrent-dd *neighbor-num*

The maximum number of neighbors of a single OSPF routing process is 5 by default.

1.13.5 Configuring the Maximum Number of Concurrent Neighbors on All Processes

1. Overview

When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which all OSPF processes can concurrently initiate or accept interaction.

2. Restrictions and Guidelines

This configuration is recommended if you want to set up an OSPF adjacency more quickly when a router is connected to a lot of other routers.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of concurrent neighbors on all processes.

router ospf max-concurrent-dd *max-neighbor*

The maximum number of neighbors of all OSPF routing processes is 10 by default.

1.14 Configuring the GR Function

1.14.1 Overview

When a GR-enabled router is restarted on the control plane, data forwarding can be still guided on the forwarding plane. In addition, actions such as neighbor relationship re-forming and route computation performed on the control

plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

1.14.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- The neighbor router must support the GR helper.
- The GR time cannot be shorter than the neighbor relationship maintenance time of the neighbor router.

1.14.3 Configuration Tasks

The configuration for enabling the GR function includes the following tasks:

(1) Enabling the GR Function

(2) (Optional) Configuring the OSPF GR Helper Function

1.14.4 Enabling the GR Function

1. Overview

The GR function is configured based on the OSPF process. You can configure different parameters for different OSPF processes based on the actual conditions. This command is used to configure the GR restarter capability of a device. The grace period is the maximum time of the entire GR process, during which link state is rebuilt so that the original state of the OSPF process is restored. After the GR period expires, OSPF exits the GR state and performs common OSPF operations.

2. Restrictions and Guidelines

- You are advised to retain the default configuration.
- The precondition for successful execution of GR and uninterrupted forwarding is that the topology remains stable. If the topology changes, OSPF quickly converges without waiting for further execution of GR, thus avoiding long-time forwarding black-hole.
- Disabling topology detection: If OSPF cannot converge in time when the topology changes during the hot standby process, forwarding black-hole may appear in a long time.
- Configuring topology detection: Forwarding may be interrupted when topology detection is enabled, but the interruption time is far shorter than that when topology detection is disabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Enable the opaque LSA processing capability.

capability opaque

The opaque LSA processing capability is enabled by default.

(5) Enable the GR function.

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

The GR capability is enabled by default.

1.14.5 Configuring the OSPF GR Helper Function

1. Overview

When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper upon receiving the Grace-LSA, and helps the neighbor to complete GR. The **disable** option indicates that the GR helper is not provided for any device that implements GR.

2. Restrictions and Guidelines

- You are advised to retain the default configuration.
- After a device becomes a GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you hope that network changes can be quickly detected during the GR process, you can configure **strict-lsa-checking** to check Type-1 to Type-5 and Type-7 LSAs that indicate the network information or **internal-lsa-checking** to check Type-1 to Type-3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (strict-lsa-checking and internal-lsa-checking) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the OSPF GR helper function.

graceful-restart helper { **disable** | **strict-lsa-checking** | **internal-lsa-checking** }

The GR helper capability is enabled by default. After the GR helper is enabled on the device, LSA changes are not checked.

1.15 Correlating OSPF with BFD

1.15.1 Overview

Once a link is faulty, OSPF can quickly detect the failure of the route. This configuration helps shorten the traffic interruption time.

1.15.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- The BFD parameters must be configured for the interface in advance.
- If BFD is configured for both a process and an interface, the interface-based configuration takes effect preferentially.
- The configuration must be performed on routers at both ends of the link.

1.15.3 Configuration Tasks

The configuration for correlating OSPF with BFD includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring BFD Correlation with OSPF on an Interface
- Configuring BFD Correlation with OSPF Globally

1.15.4 Configuring BFD Correlation with OSPF on an Interface

1. Overview

Correlating OSPF with BFD on a specified interface can quickly detect the interface fault and accelerate OSPF convergence.

2. Restrictions and Guidelines

- The BFD configured on an interface takes precedence over that configured in OSPF process configuration mode.
- Based on the actual environment, you can run the **ip ospf bfd** command to enable BFD on a specified interface for link detection, or run the **bfd all-interfaces** command in OSPF process configuration mode to enable BFD on all interfaces of the OSPF process, or run the **ip ospf bfd disable** command to disable BFD on a specified interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Correlate OSPF with BFD on an interface.

ip ospf bfd [**disable**]

By default, the BFD function is disabled on an interface, and the BFD configuration is subject to that configured in RIP process configuration mode.

1.15.5 Configuring BFD Correlation with OSPF Globally

1. Overview

OSPF dynamically discovers neighbors through the hello packets. After OSPF enables the BFD function, a BFD session will be set up to achieve the full adjacency, and the BFD mechanism is used to detect the neighbor state. Once a neighbor failure is detected through BFD, OSPF performs network convergence immediately.

2. Restrictions and Guidelines

You can also run the **ip ospf bfd** [**disable**] command in interface configuration mode to enable or disable the BFD function on a specified interface, and this configuration takes precedence over the **bfd all-interfaces** command used in OSPF process configuration mode.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Enter correlation with BFD in OSPF configuration mode.

bfd all-interfaces

By default, the BFD function is disabled on all the interfaces.

1.16 Enabling Overflow

1.16.1 Overview

New routes are not loaded to routers when the router memory is insufficient or the usage of the database space reaches the upper limit.

1.16.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- After a router enters the overflow state, you can run the **clear ip ospf process** command, or stop and then restart the OSPF protocol to exit the overflow state.

1.16.3 Configuration Tasks

The configuration of enabling overflow includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring the Memory Overflow Function
- Configuring the Database Overflow Function
- Configuring the External LSA Database Overflow Function

1.16.4 Configuring the Memory Overflow Function

1. Overview

The OSPF process enters the overflow state to discard newly-learned external routes. This behavior can effectively prevent the memory usage from increasing.

2. Restrictions and Guidelines

- This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.
- After the overflow function is enabled, the OSPF process enters the overflow state and discards newly-learned external routes, which may cause a routing loop on the entire network. To reduce the occurrence probability of this problem, OSPF generates a default route to the null interface, and this route always exists in the overflow state.
- You can run the **clear ip ospf process** command to reset the OSPF process so that the OSPF process can exit the overflow state. You can run the **no** form of the command to prevent the OSPF process from entering the overflow state when the memory is insufficient. This, however, may lead to over-consumption of the memory resource, after which the OSPF process will stop and delete all the learned routes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the memory overflow function.

overflow memory-lack

By default, the OSPF process is allowed to enter the overflow state when the memory is insufficient.

1.16.5 Configuring the Database Overflow Function

1. Overview

This function controls the maximum number of routes in LSDB to avoid abnormal operation of a router due to insufficient memory.

2. Restrictions and Guidelines

This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the database overflow function.

overflow database *max-lsa* [**hard** | **soft**]

The maximum number of LSAs is not configured by default.

1.16.6 Configuring the External LSA Database Overflow Function

1. Overview

This function controls the maximum number of external routes in LSDB to avoid abnormal operation of a router due to insufficient memory.

2. Restrictions and Guidelines

- This configuration is recommended if the ASBR introduces a large number of external routes and the router memory may be insufficient.
- When using the overflow function, ensure that the same *max-dbsize* is configured on all routers in the OSPF backbone area and common areas; otherwise, the following problems may occur:
  - The LSDBs throughout the network are inconsistent, and the neighbor relationship fails to reach the full state.

- Routes are incorrect, including routing loops.
- AS external LSAs are frequently retransmitted.

- If the maximum number of external LSAs is set, when the number of external LSAs exceeds the maximum, the normal state will not be restored.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the external LSA database overflow function.

overflow database external *max-dbsize wait-time*

The maximum number of external LSAs is not configured by default.

1.17 Configuring VPN Extended Feature of OSPF

1.17.1 Overview

When OSPF is enabled on a VPN client network, OSPF runs between the PE and CE to simplify the configuration and management of CE.

1.17.2 Restrictions and Guidelines

The router ID of Label Distribution Protocol (LDP) must consist of 32 bits.

1.17.3 Configuration Tasks

The configuration of VPN extended feature of OSPF includes the following tasks:

- (Optional) Configuring Domain ID
- (Optional) Configuring a Sham Link
- (Optional) Configuring a Domain Label
- (Optional) Disabling Loop Detection for a VRF OSPF ProcessDisabling Loop Detection for a VRF OSPF Process
- (Optional) Configuring Extcommunity Attribute for a VPN Route
- Disabling Loop Detection Using the DN Bit of LSA
- Disabling Loop Detection Using the Route Tag of LSA

1.17.4 Configuring Domain ID

1. Overview

Domain ID is used to indicate the domain information of an OSPF process.

A VRF OSPF process can be configured with multiple domain IDs, but only one is the primary domain ID, and the remaining ones are secondary domain IDs. An OSPF route is converted into a VPN route for advertising, and only the primary domain ID is included in a VPN route.

2. Restrictions and Guidelines

- This function takes effect only for the OSPF process associated with VRF.
- The domain IDs of different VRF OSPF processes do not influence each other, and can be configured the same. However, the VRF OSPF processes that belong to the same VPN must be configured with the same domain ID to ensure the correctness of route advertising.
- You are advised to configure all the VRF OSPF processes that belong to the same VPN with the same domain ID.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Configure a domain ID.

domain-id { *ipv4-address* [**secondary**] | **null** | **type** { **0005** | **0105** | **0205** | **8005** } **value** *hex-value* [**secondary**] }

By default, the domain ID value of an OSPF process is **null**, and the type value is 0x0005.

1.17.5 Configuring a Domain Label

1. Overview

If a VPN site is connected to multiple PEs, the VPN route is learned from the PE through MP-BGP. If the route is advertised to the VPN site through a Type-5 or Type-7 LSA, it may be learned and advertised by other PE routers connected to the VPN site, which may cause a loop. To prevent the preceding loop, the VRF OSPF processes connected to the same VPN site on the PEs are configured with the same VPN route tag. When a VRF OSPF

process sends a Type-5 or Type-7 LSA to a VPN site, the VPN route tag information will also be attached to the LSA. When other PE sites receive such a Type-5 or Type-7 LSA, if they detect that the VPN route tag in the LSA is consistent with that of the local OSPF process, the LSA will not participate in the OSPF computation. Generally, the OSPF processes belonging to the same VPN site are configured with the same tag value.

The VPN route tag occupies four bytes in an OSPF packet. If a VRF OSPF process is not configured with this command, when the OSPF process advertises a Type-5 or Type-7 LSA, the first two bytes of the VPN route tag are set to 0xD000 by default, and the last two bytes are the AS number of local BGP. For example, if the AS number of the local BGP is 1, the hexadecimal form of the VPN route tag is 0xD0000001.

2. Restrictions and Guidelines

This function takes effect only for the OSPF process associated with VRF and BGP redistributed routes.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Configure a VPN route tag.

domain-tag *tag*

By default, the default value of a VRF OSPF process is the AS number of the local BGP protocol.

1.17.6 Configuring a Sham Link

1. Overview

A sham link is used in an environment with backdoor links between VPN sites. If you still want VPN data to be transmitted through the MPLS backbone network in this case, you can establish a sham link between the VRF OSPF processes of two PEs. The VRF OSPF processes of two PEs can set up an OSPF neighbor relationship through the sham link and distribute LSA packets on the sham link.

2. Restrictions and Guidelines

- The area ID of sham link configured for the two PEs must be consistent.
- The combination of source address and destination address of a sham link configured on one PE must be equal to the combination of destination address and source address of a sham link configured on the other PE.

- Both the source address and destination address used to establish a sham link on the PEs must be a 32-bit loopback address bound to the corresponding VRF.
- Since the OSPF route advertised through a sham link has no VPN label, the route cannot be used for forwarding. Actually packets are still forwarded through the BGP VPNv4 route. Therefore, in the actual configuration, you must ensure that the route advertised through the sham link will also be learned through MP-BGP.
- The source address for establishing the sham link must participate in the BGP VPNv4 route advertisement, but cannot join the calculation of VRF OSPF process.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Configure a sham link.

area *area-id* **sham-link** *source-ipv4-address destination-ipv4-address* [[**authentication** [**keychain** *kechain-name* | **message-digest** | **null**] | **cost** *number* | **dead-interval** ***dead-interval*** | **hello-interval** *hello-interval* | **retransmit-interval** *retransmit-interval* | **transmit-delay** *transmit-delay*] * | **authentication-key** [**0** | **7**] *key* | **message-digest-key** *key-id* **md5** [**0** | **7**] *key*]

No sham link is configured by default.

1.17.7 Disabling Loop Detection for a VRF OSPF Process

1. Overview

Loop detection of OSPF processes aims to prevent possible loop of VPN routes in propagation.

2. Restrictions and Guidelines

- By default, the VRF OSPF process supports the PE-CE OSPF features (that is, conversion from domain ID to LSA, to DN bits, and to VPN route tag). If you do not want a VRF OSPF process to support the PE-CE OSPF features, disable the PE-CE OSPF features by running the **capability vrf-lite** command.
- This command takes effect only for the OSPF process associated with VRF.
- In some application scenarios, you may need to disable the loop detection function of VRF OSPF processes. For example, VPN users use MCE devices to exchange VPN routes with PEs, if the OSPF protocol runs between MCEs and PEs to exchange VPN routes, to enable the VPN site to learn the routes of other VPN sites, you need

to run the **capability vrf-lite** command to disable the loop detection function of VRF OSPF processes on the MCE device.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Configure capability vrf-lite.

capability vrf-lite [**auto**]

By default, the automatic judging function of support to loop detection is enabled for the OSPF processes associated with VRF.

1.17.8 Configuring Extcommunity Attribute for a VPN Route

1. Overview

When an OSPF route of VRF forms a VPN route, the Router-ID and Router-Type of the OSPF process will also be carried in the extcommunity attribute of the VPN route. To ensure compatibility with the implementations of different vendors, you can manually modify the Router-ID and Router-Type.

2. Restrictions and Guidelines

- When OSPF routes are redistributed to BGP to form VPN routes, the extcommunity attributes of OSPF routes, including the extcommunity attributes of **router-id** and **route-type**, will also be attached. By default, the extcommunity attribute type of **router-id** is 0x0107, and the extcommunity attribute of **route-type** is 0x0306. You can also use commands to manually configure the extcommunity attributes of **router-id** and **route-type**.
- This function takes effect only for the OSPF process associated with VRF.
- Configuring the type of **router-id** aims to ensure compatibility with the implementations of different vendors. For example, some vendors support the **router-id** type “0x0107” only. In the case of interconnection with the devices of these vendors, you need to set the type of **router-id** to 0x0107 by using the **extcommunity-type** command.
- Configuring the type of **router-type** aims to ensure compatibility with the implementations of different vendors. For example, some vendors support the **route-type** “0x8000” only. In the case of interconnection with the devices of these vendors, you need to set **route-type** to 0x8000 by using the **extcommunity-type** command.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Configure **extcommunity-type**.

extcommunity-type { **router-id** { **0107 | 8001** } | **route-type** { **0306** | **8000** } }

By default, the type of **router-id** is 0107, and the type of **route-type** is 0306.

1.17.9 Disabling Loop Detection Using the DN Bit of LSA

1. Overview

In the CE dual-homing scenario of L3VPN, loop is avoided by suppressing the route computation of DN bit between PEs. However, in a specific scenario, PEs may be allowed to learn routes from each other without generating any loops. In this case, check of the DN bit can be cancelled by configuring this command. When a PE device is connected to an MCE device, the MCE device needs to calculate the route advertised by the PE and the DN bit will not be checked. Type-3, Type-5, and Type-7 LSAs of OSPF can all carry a DN bit.

2. Restrictions and Guidelines

This function takes effect only for the OSPF process associated with VRF.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Disable loop detection using the DN bit of LSA.

disable-dn-bit-check [**summary | ase | nssa**]

The DN bit loop detection function of LSA is enabled by default.

1.17.10 Disabling Loop Detection Using the Route Tag of LSA

1. Overview

In the CE dual-homing scenario of L3VPN, when the LSA route tag received by a PE is the same as its route tag, the route is not calculated, thus avoiding a loop. In a specific scenario, PEs are allowed to learn routes from each other without generating any loops. In this case, you can set different route tags for multiple PEs, or set to disable route tag check. When a PE device is connected to an MCE device, the MCE device needs to calculate the route advertised by the PE and the route tag will not be checked. Type-5 and Type-7 LSAs of OSPF can carry a route tag.

2. Restrictions and Guidelines

This command takes effect only for the OSPF process associated with VRF.

3. Prerequisites

Before configuring the VPN feature, complete the VRF configuration.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *ospf-id* **vrf** *vrf-name*

(4) Disable loop detection using the route tag of LSA.

disable-tag-check

The loop detection function using the route tag of LSA is enabled by default.

1.18 Configuring Network Management Functions

1.18.1 Overview

Use the network management software to manage OSPF parameters and monitor the OSPF running status.

1.18.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- You must enable the MIB function of the SNMP-Server before enabling the OSPF MIB function.

- You must enable the Trap function of the SNMP-Server before enabling the OSPF Trap function.
- You must enable the logging function of the device before outputting the OSPF logs.

1.18.3 Configuration Tasks

The configuration of network management functions includes the following tasks:

- Binding the MIB with an OSPF Process
- Configuring the Trap Function
- Configuring the Logging Function

1.18.4 Binding the MIB with an OSPF Process

1. Overview

This configuration is required if you want to use the network management software to manage parameters of a specified OSPF process.

2. Restrictions and Guidelines

- The OSPFv2 MIB does not have the OSPFv2 process information. Therefore, you must perform operations on a single OSPFv2 process through SNMP. By default, the OSPFv2 MIB is bound with the OSPFv2 process with the smallest process ID, and all user operations take effect on this process.
- If you hope to perform operations on a specified OSPFv2 process through SNMP, run this command to bind the MIB to the process.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Bind the MIB with an OSPF process.

enable mib-binding

By default, the MIB is bound to the OSPFv2 process with the minimum process ID.

1.18.5 Configuring the Trap Function

1. Overview

This configuration is required if you want to use the network management software to monitor the OSPF running status.

2. Restrictions and Guidelines

- The function configured by this command is restricted by the **snmp-server** command. You need to configure the **snmp-server enable traps ospf** command and then the **enable traps** command before the corresponding OSPF trap can be correctly sent out.
- This command is not restricted by the MIB bound to the process. The trap switch can be enabled concurrently for different processes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the trap function.

enable traps [**error** [**IfAuthFailure** | **IfConfigError** | **IfRxBadPacket** | **VirtIfAuthFailure** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **lsa** [**LsdbApproachOverflow** | **LsdbOverflow** | **MaxAgeLsa** | **OriginateLsa**] | **retransmit** [**IfTxRetransmit** | **VirtIfTxRetransmit**] | **state-change** [**IfStateChange** | **NbrRestartHelperStatusChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **RestartStatusChange** | **VirtIfStateChange** | **VirtNbrRestartHelperStatusChange** | **VirtNbrStateChange**]]

The trap message sending function is disabled by default.

1.18.6 Configuring the Logging Function

1. Overview

This function outputs the relevant log records so that the related information can be analyzed and found easily.

2. Restrictions and Guidelines

You are advised to retain the default configuration. If you want to reduce the log output, disable this function.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the logging function.

log-adj-changes [**detail**]

The logging function is enabled by default, without the **detail** parameter. The log records the log information of the following four types of events only: the adjacency reaches the full state; the adjacency leaves the full state; the adjacency reaches the down state; the adjacency leaves the down state.

1.19 Enabling NSR

1.19.1 Overview

During an active/standby switchover of devices in distributed (with the independent active/standby modular engine) or VSU mode, data forwarding continues and is not interrupted.

1.19.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- You are advised to retain the default configuration.
- This command is used to enable the NSR function. For the same OSPF process, either NSR or GR is enabled because they are mutually exclusive. Nevertheless, when NSR is enabled, the GR helper capability is supported.
- The switchover of devices in a distributed or VSU mode takes a period of time. If the OSPF neighbor keepalive duration is shorter than the switchover duration, the OSPF neighbor relationship with the neighbor device is removed, and services are interrupted during the switchover. Therefore, it is recommended that the OSPF neighbor keepalive duration be no smaller than the default value when the NSR function is enabled. It is recommended that the fast hello function be disabled because when it is enabled, the OSPF neighbor keepalive duration is less than 1s.

1.19.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Enable the NSR function.

nsr

The NSR function is disabled by default.

1.20 Enabling the iSPF Feature

1.20.1 Overview

OSPF adopts the iSPF algorithm to compute a network topology. The iSPF function is generally used on a large-sized network to ease the pressure on router processors.

1.20.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- This configuration is recommended if you hope to accelerate route convergence in a single area with more than 100 routers.
- This configuration is performed on all routers in the area.
- After iSPF is enabled, OSPF will use the iSPF algorithm to compute the network topology. That is, after the network topology changes, OSPF corrects only the nodes affected by the topological change, instead of re-building the entire SPT.

1.20.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the **i**SPF feature.

ispf enable

The iSPF feature is disabled by default.

1.21 Configuring to Disable MTU Verification

1.21.1 Overview

On receiving the database description packet, OSPF checks whether the MTU of the interface on the neighbor is the same as the MTU of its own interface. If the interface MTU specified in the received database description packet is greater than the MTU of the local interface, the adjacency cannot be set up. To resolve this problem, you can disable MTU verification.

1.21.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.

- You are advised to retain the default configuration.
- This configuration is performed on two routers with different interface MTUs.

1.21.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure to disable MTU verification.

ip ospf mtu-ignore

The MTU verification function is disabled by default.

1.22 Configuring a Super VLAN to Enable OSPF

1.22.1 Overview

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when OSPF multicast packets are sent over a super VLAN containing multiple sub VLANs, the OSPF multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing protocol flapping. In certain application scenarios in which OSPF packets need to be sent over a super VLAN, the packets only need to be sent over a sub VLAN of the super VLAN. In this case, you can run the command to specify a sub VLAN to avoid the neighbor flapping caused by a device processing bottleneck.

1.22.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- The designated sub VLAN must be connected to neighbors.

1.22.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface vlan *vlan-id*

(4) Configure the **subvlan** feature.

ip ospf subvlan *vlan-id*

The OSPF function is not configured for a super VLAN by default.

1.23 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

You can run the **clear** commands to clear information.

Caution

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

Run the **debug** command to output debugging information.

Caution

When the **debug** command is used to output debugging information, system resources are occupied. Therefore, disable the debugging function immediately after use.

Table 1-9 OSPF Monitoring

Command	Purpose
show ip ospf [*process-id*]	Displays the OSPF process configuration information.
show ip ospf [*process-id*] **border-routers**	Displays the OSPF internal routing table (the routes to ABRs and ASBRs).
show ip ospf [*process-id area-id*] **database** [{ **asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary** }] [{ **adv-router** *ip-address* | **self-originate** } | *link-state-id* | **brief**] [**database-summary** | **max-age** | **detail**]	Displays the information of the OSPF LSDB.
show ip ospf [*process-id*] **interface** [*interface-type interface-number* | **brief**]	Displays the OSPF-enabled interface.
show ipv6 ospf [*process- id*] **keepalive** [**process** | **area** [*area-id*] | **interface** [*interface-type interface-number*] [**with-clear** | **nbr**] | [**virtual-link** | **send-queue** | **recv-queue**] [**with-clear**]]	Displays the OSPFv3 keepalive thread information.

Command	Purpose
show ip ospf [*process-id*] **neighbor** [[*interface-type interface-number* | *neighbor-id*] * [**detail**] | **statistics**]	Displays the neighbor list of an OSPF process.
show ip ospf [*process-id*] **route** [**count**]	Displays the OSPF routing table.
show ip ospf [*process-id*] **sham-links** [**area** *area-id*]	Displays the sham link information of an OSPF process.
show ip ospf [*process-id*] **spf**	Displays the number of times SPT is computed in the OSPF area.
show ip ospf [*process-id*] **summary-address**	Displays the summarized route of OSPF redistributed routes.
show ip ospf [*process-id* [*area-id*]] **topology** [**adv-router** *adv-router-id* [*router-id*] | **self-originate** [*router-id*]]	Displays the OSPF network topology information.
show ip ospf [*process-id*] **virtual-links** [*ip-address*]	Displays OSPF virtual links.
show running-config router ospf	Displays the OSPF configuration.
clear ip ospf [*process-id*] **process**	Clears and resets an OSPF process.
debug ip ospf events [**abr** | **asbr** | **lsa** | **nssa** | **os** | **restart** | **router** | **slink** | **vlink**]	Debugs OSPF events.
debug ip ospf ifsm [**events** | **status** | **timers**]	Debugs OSPF interfaces.
debug ip ospf nfsm [**events** | **status** | **timers**]	Debugs OSPF neighbors.
debug ip ospf nsm [**interface** | **redistribute** | **route**]	Debugs the OSPF NSM.
debug ip ospf lsa [**flooding** | **generate** | **install** | **maxage** | **refresh**]	Debugs OSPF LSAs.
debug ip ospf packet [**dd | detail** | **hello** | **ls-ack** | **ls-request** | **ls-update** | **recv** | **send**]	Debugs OSPF packets.
debug ip ospf route [**ase** | **ia** | **install** | **spf** | **time**]	Debugs OSPF routes.

1.24 Configuration Examples

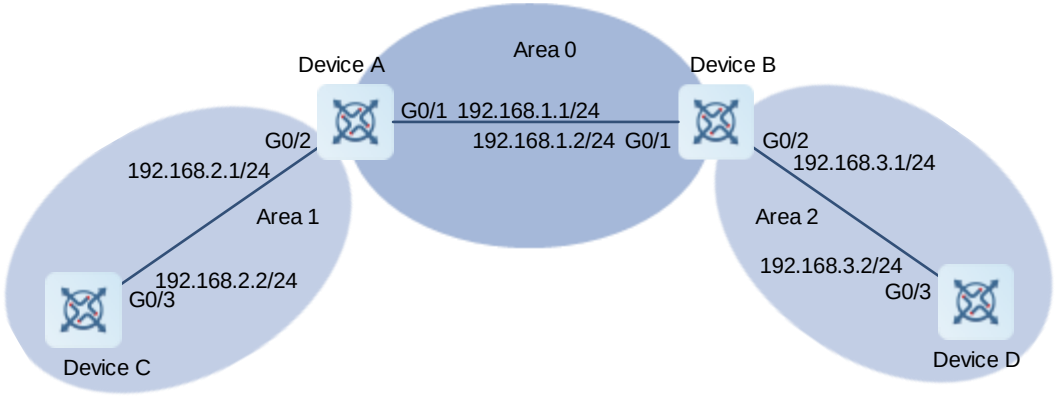
1.24.1 Configuring Basic Functions of OSPF

1. Requirements

OSPF is enabled on all the devices, and three areas are defined in total. Device A and device B are used as ABR forwarding inter-area routes so as to implement the interworking between all networks. After configuration, all devices can learn the routing of all network segments in the AS, and the neighbor relationships are correct.

2. Topology

Figure 1-14 Topology for Configuring Basic Functions of OSPF



3. Notes

- Configure interface IP addresses on all the devices.
- Enable the IPv4 unicast routing function on all the devices. (This function is enabled by default.)
- Configure the OSPF processes and router IDs on all the devices.
- Configure interface configuration OSPF on all the devices.

4. Procedure

(1) Configure interface IP addresses on all the devices.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/1)# exit
```

```
Device A(config)# interface GigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/2)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ip address 192.168.3.1 255.255.255.0
Device B(config-if-GigabitEthernet 0/2)# exit
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface GigabitEthernet 0/3
Device C(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0
Device C(config-if-GigabitEthernet 0/3)# exit
```

Configure Device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# interface GigabitEthernet 0/3
Device D(config-if-GigabitEthernet 0/3)# ip address 192.168.3.2 255.255.255.0
Device D(config-if-GigabitEthernet 0/3)# exit
```

(2) Configure the OSPF process, router ID, and the interface configuration OSPF.

Configure Device A.

```
Device A(config)# router ospf 1
Device A(config-router)# router-id 192.168.1.1
Device A(config-router)# network 192.168.1.0 0.0.0.255 area 0
Device A(config-router)# network 192.168.2.0 0.0.0.255 area 1
```

Configure Device B.

```
Device B(config)# router ospf 1
Device B(config-router)# router-id 192.168.1.2
Device B(config-router)# network 192.168.1.0 0.0.0.255 area 0
Device B(config-router)# network 192.168.3.0 0.0.0.255 area 2
```

Configure Device C.

```
Device C(config)# router ospf 1
Device C(config-router)# router-id 192.168.2.2
Device C(config-router)# network 192.168.2.0 0.0.0.255 area 1
```

Configure Device D.

```
Device D(config)# router ospf 1
Device D(config-router)# router-id 192.168.3.2
Device D(config-router)# network 192.168.3.0 0.0.0.255 area 2
```

5. Verification

(1) Check the OSPF neighbor and route of Device A.

Check the OSPF route of Device A.

```
Device A# show ip route ospf
O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
```

Check the neighbor information of Device A.

```
Device A# show ip ospf neighbor
OSPF process 1, 2 Neighbors, 2 is Full:
Neighbor ID   Pri   State     Dead Time   Address      Interface
192.168.1.2   1     Full/DR   00:00:40    192.168.1.2   GigabitEthernet 0/1
192.168.2.2   1     Full/BDR  00:00:34    192.168.2.2   GigabitEthernet 0/2
```

(2) Check the OSPF neighbor and route of Device B.

Check the OSPF route of Device B.

```
Device B# show ip route ospf
O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
```

Check the neighbor information of Device B.

```
Device B# show ip ospf neighbor
OSPF process 1, 2 Neighbors, 2 is Full:
Neighbor ID   Pri   State     Dead Time   Address      Interface
192.168.1.1   1     Full/BDR  00:00:32    192.168.1.1   GigabitEthernet 0/1
192.168.3.2   1     Full/BDR  00:00:30    192.168.3.2   GigabitEthernet 0/2
```

(3) Check the OSPF neighbor and route of Device C.

Check the OSPF route of Device C.

```
Device C# show ip route ospf
O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
O IA 192.168.3.0/24 [110/3] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
```

Check the neighbor information of Device C.

```
Device C# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID   Pri   State     Dead Time   Address      Interface
192.168.1.1   1     Full/BDR  00:00:32    192.168.2.1   GigabitEthernet 0/3
```

(4) Check the OSPF neighbor and route of Device D.

Check the OSPF route of Device D.

```
Device D# show ip route ospf
O IA 192.168.1.0/24 [110/2] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3
O IA 192.168.2.0/24 [110/3] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3
```

Check the neighbor information of Device D.

```
Device D# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID   Pri   State     Dead Time   Address      Interface
192.168.1.2   1    Full/BDR   00:00:30    192.168.3.1   GigabitEthernet 0/3
```

(5) Ping 192.168.2.2 on Device D. The network is reachable.

```
Device D# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 ip address 192.168.2.1 255.255.255.0
!
router ospf 1
 router-id 192.168.1.1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 1
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
 ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
ip address 192.168.3.1 255.255.255.0
!
router ospf 1
 router-id 192.168.1.2
 network 192.168.1.0 0.0.0.255 area 0
! network 192.168.3.0 0.0.0.255 area 2
```

- Device C configuration file

```
!
interface GigabitEthernet 0/3
 ip address 192.168.2.2 255.255.255.0
!
router ospf 1
 router-id 192.168.2.2
 network 192.168.2.0 0.0.0.255 area 1
!
```

- Device D configuration file

```
!
interface GigabitEthernet 0/3
 ip address 192.168.3.2 255.255.255.0
!
router ospf 1
 router-id 192.168.3.2
 network 192.168.3.0 0.0.0.255 area 2
!
```

7. Common Errors

- OSPF cannot be enabled because the IP unicast routing function is disabled.
- The network segment configured by the **network** command does not include the interface IP addresses.
- The area IDs configured for adjacent interfaces are inconsistent.
- The same router ID is configured on multiple devices, resulting in a router ID conflict.
- The same interface IP address is configured on multiple devices, resulting in a running error of the OSPF network.

1.24.2 Configuring a Stub Area

1. Requirements

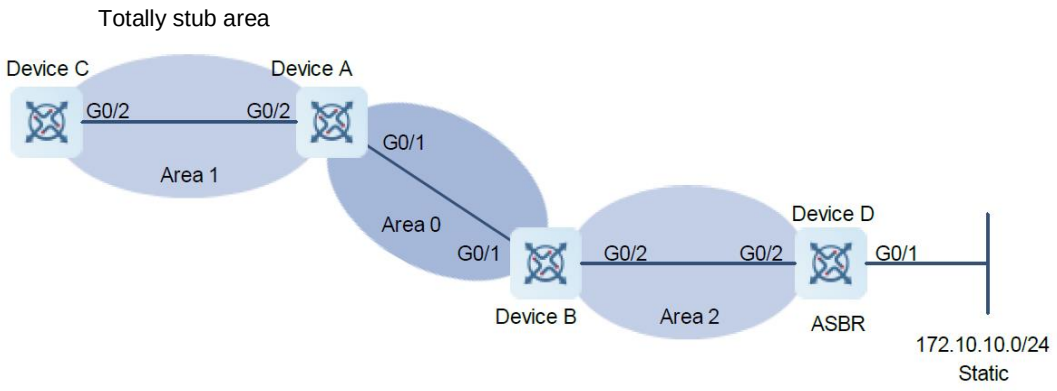
Device A, Device B, Device C, and Device D are interconnected through the OSPF routing protocol.

As ABRs, Device A and Device B are responsible for the routing information transfer between OSPF areas, and Device D functions as an ASBR to introduce the external static route.

To reduce the number of LSAs in Area 1 and save the device performance, Area 1 is configured as a totally stub area.

2. Topology

Figure 1-15 Topology for a Stub Area



3. Notes

- Configure interface IP addresses for all devices (omitted).
- Configure OSPF basic functions on all devices (omitted).
- Introduce an external static route to Device D.
- Configure Area 1 as a stub area on Device A and Device C.

4. Procedure

(1) Introduce an external static route to Device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# router ospf 1
Device D(config-router)# redistribute static subnets
```

(2) Configure Area 1 as a stub area on Device A and Device C.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# router ospf 1
Device A(config-router)# area 1 stub no-summary
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# router ospf 1
Device C(config-router)# area 1 stub
```

5. Verification

On Device C, run the **show ip route ospf** command to display the routing table. Verify that there is only one default inter-area route, and no external static route is introduced from Device D.

```
Device C# show ip route ospf
O*IA 0.0.0.0/0 [110/2] via 192.168.2.1, 00:30:53, GigabitEthernet 0/2
```

6. Configuration Files

- Device A configuration file

```
!
router ospf 1
 area 1 stub no-summary
!
```

- Device C configuration file

```
!
router ospf 1
 area 1 stub
!
```

- Device D configuration file

```
!
router ospf 1
 redistribute static subnets
!
```

1.24.3 Configuring an NSSA

1. Requirements

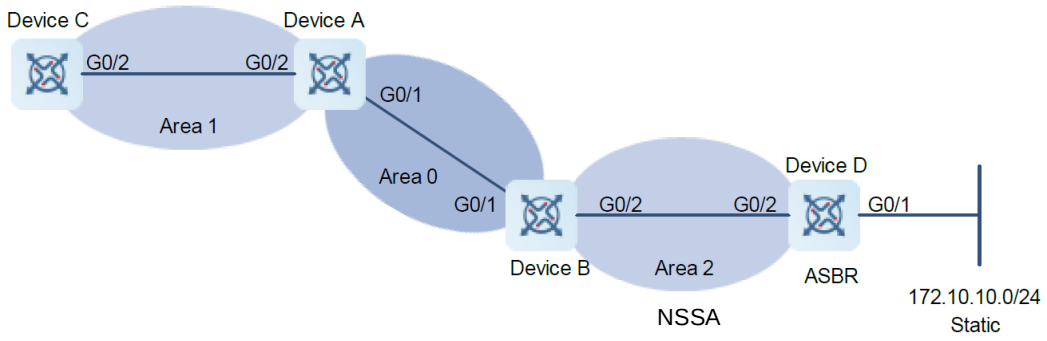
Device A, Device B, Device C, and Device D are interconnected through the OSPF routing protocol.

As ABRs, Device A and Device B are responsible for the routing information transfer between OSPF areas, and Device D functions as an ASBR to introduce the external static route.

To reduce the number of LSAs in Area 2 and save the device performance, Area 2 is configured as an NSSA.

2. Topology

Figure 1-16 Topology for an NSSA



3. Notes

- Configure interface IP addresses for all devices (omitted).
- Configure OSPF basic functions on all devices (omitted).
- Introduce an external static route to Device D.
- Configure Area 2 as NSSA on Device B and Device D.

4. Procedure

(1) Configure a static route for Device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# ip route 172.10.10.0 255.255.255.0 192.168.6.2
```

(2) Introduce an external static route to Device D.

```
Device D(config)# router ospf 1
Device D(config-router)# redistribute static subnets
```

(3) Configure Area 2 as NSSA on Device B and Device D.

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# router ospf 1
Device B(config-router)# area 2 nssa
```

Configure Device D.

```
Device D(config-router)# area 2 nssa
```

5. Verification

On Device D, check the Type-7 LSAs generated from 172.10.10.0/24.

```
Device D# show ip ospf database nssa-external
          OSPF Router with ID (192.168.6.2) (Process ID 1)
             NSSA-external Link States (Area 0.0.0.1 [NSSA])
  LS age: 61
  Options: 0x8 (-|-|-|-|N/P|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 172.10.10.0 (External Network Number For NSSA)
  Advertising Router: 192.168.6.2
  LS Seq Number: 80000001
  Checksum: 0xc8f8
  Length: 36
  Network Mask: /24
       Metric Type: 2 (Larger than any link state path)
       TOS: 0
       Metric: 20
       NSSA: Forward Address: 192.168.6.2
       External Route Tag: 0
```

On Device B, verify that Type-5 and Type-7 LSAs are generated from 172.10.10.0/24.

```
Device B# show ip ospf database nssa-external
          OSPF Router with ID (192.168.3.1) (Process ID 1)
             NSSA-external Link States (Area 0.0.0.1 [NSSA])
  LS age: 314
  Options: 0x8 (-|-|-|-|N/P|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 172.10.10.0 (External Network Number For NSSA)
  Advertising Router: 192.168.6.2
  LS Seq Number: 80000001
  Checksum: 0xc8f8
  Length: 36
  Network Mask: /24
       Metric Type: 2 (Larger than any link state path)
       TOS: 0
       Metric: 20
       NSSA: Forward Address: 192.168.6.2
       External Route Tag: 0
```

On Device B, check the Type-N2 routes generated from 172.10.10.0/24.

```
Device B# show ip ospf database external
          OSPF Router with ID (192.168.3.1) (Process ID 1)
             AS External Link States
```

```
LS age: 875
Options: 0x2 (-|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 172.10.10.0 (External Network Number)
Advertising Router: 192.168.3.1
LS Seq Number: 80000001
Checksum: 0xd0d3
Length: 36
Network Mask: /24
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 20
     Forward Address: 192.168.6.2
     External Route Tag: 0
```

6. Configuration Files

- Device B configuration file

```
!
router ospf 1
 area 2 nssa
!
```

- Device D configuration file

```
!
ip route 172.10.10.0 255.255.255.0 192.168.6.2
!
router ospf 1
 redistribute static subnets
 area 2 nssa
!
```

7. Common Errors

- Configurations of the area type are inconsistent on devices in the same area.
- External routes cannot be introduced because route redistribution is configured on a device in the stub area.

1.24.4 Correlating OSPF Process with BFD

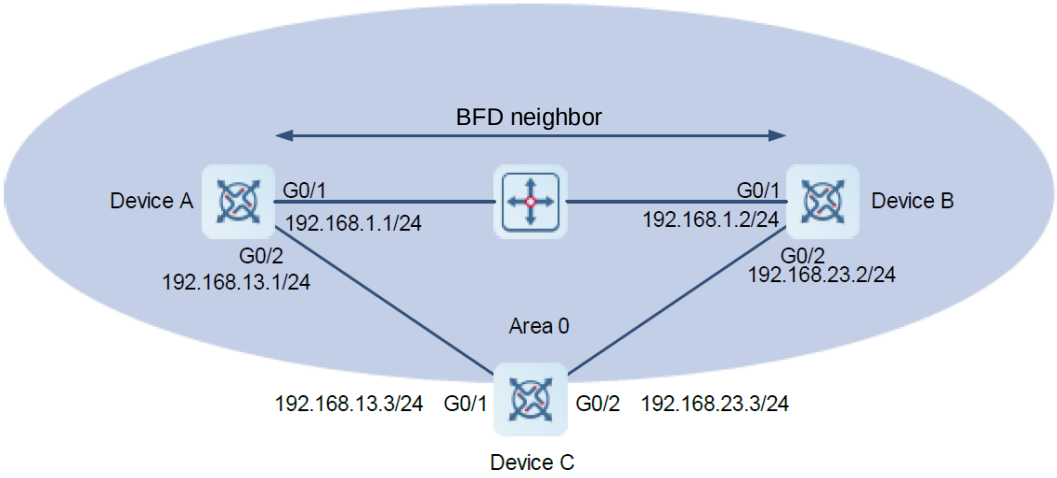
1. Requirements

Device A, Device B, and Device C implement internetworking by running OSPFv2.

Device A and Device B use a switch as the primary link. When the switch or the link connected to it fails, BFD can quickly detect the failure and switch to Device C for communication.

2. Topology

Figure 1-17 Topology for Correlating an OSPF Process with BFD



3. Notes

- Configure interface IP addresses for all devices (omitted).
- Configure OSPF basic functions on all devices (omitted).
- Configure the BFD parameters for the interfaces of all devices.
- Correlate OSPF with BFD on all the devices.

4. Procedure

(1) Configure BFD parameters for the interfaces of all devices.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier 5
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface GigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# bfd interval 200 min_rx 200 multiplier 5
Device A(config-if-GigabitEthernet 0/2)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier 5
```

```
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# bfd interval 200 min_rx 200 multiplier 5
Device B(config-if-GigabitEthernet 0/2)# exit
```

(2) Correlate OSPF with BFD on all the devices.

Configure Device A.

```
Device A(config)# router ospf 1
Device A(config-router)# bfd all-interfaces
```

Configure Device B.

```
Device B(config)# router ospf 1
Device B(config-router)# bfd all-interfaces
```

5. Verification

On Device A, verify that correlating OSPF with BFD is up.

```
Device A# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID    Pri   State        BFD State  Dead Time   Address        Interface
192.168.1.2      1   Full/BDR      Up        00:00:40   192.168.1.2
GigabitEthernet 0/1
192.168.13.3      1   Full/BDR      Up        00:00:40   192.168.13.3
GigabitEthernet 0/2
```

On Device B, verify that correlating OSPF with BFD is up.

```
Device B# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID    Pri   State        BFD State  Dead Time   Address        Interface
192.168.1.1      1   Full/BDR      Up        00:00:40   192.168.1.1
GigabitEthernet 0/1
192.168.13.3      1   Full/BDR      Up        00:00:40   192.168.23.3
GigabitEthernet 0/2
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 bfd interval 200 min_rx 200 multiplier 5
!
interface GigabitEthernet 0/2
 bfd interval 200 min_rx 200 multiplier 5
!
router ospf 1
```

```
 bfd all-interfaces
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
 bfd interval 200 min_rx 200 multiplier 5
!
interface GigabitEthernet 0/2
 bfd interval 200 min_rx 200 multiplier 5
!
router ospf 1
 bfd all-interfaces
!
```

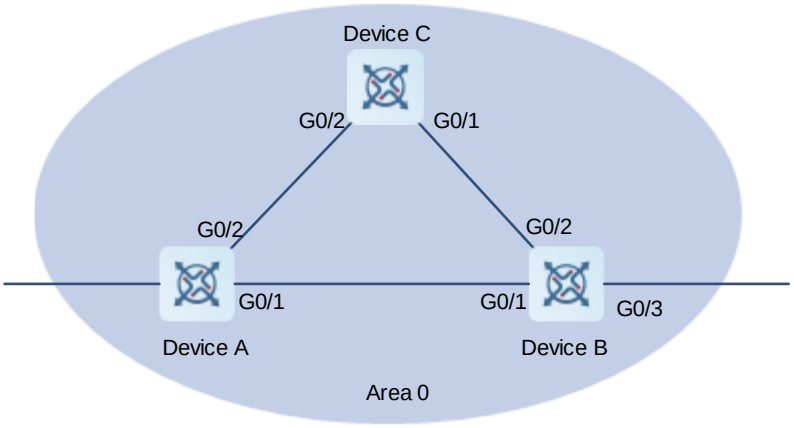
1.24.5 Configuring Fast Reroute

1. Requirements

Devices A, B, and C belong to the same OSPF area, and any two of them implement internetworking through the OSPF protocol. When a link of Device A fails, the service can be quickly switched to the backup link. The handover delay should be reduced as much as possible.

2. Topology

Figure 1-18 Topology for Fast Reroute



3. Notes

- Configure fast reroute on Device A.
- Configure **carrier-delay 0** on the interfaces on Device A.

4. Procedure

(1) Configure interface IP addresses for all devices (omitted).

(2) Configure OSPF basic functions on all devices (omitted).

(3) Configure fast reroute on Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# router ospf 1
Device A(config-router)# fast-reroute lfa
Device A(config-router)# exit
```

(4) Configure carrier-delay 0 on all the interfaces of Device A.

```
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# carrier-delay 0
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface GigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# carrier-delay 0
```

5. Verification

On Device A, check the routing table to verify that a backup route exists for the entry 192.168.4.0/24.

```
Device A# show ip route fast-reroute  | begin 192.168.4.0
O  192.168.4.0/24 [ma] via 192.168.1.2, 00:39:28, GigabitEthernet 0/1
                 [b] via 192.168.2.2, 00:39:28, GigabitEthernet 0/2
```

6. Configuration Files

Device A configuration file

```
!
router ospf 1
fast-reroute lfa
!
interface GigabitEthernet 0/1
carrier-delay 0
!
interface GigabitEthernet 0/2
 carrier-delay 0
!
```

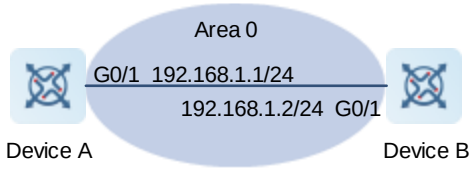
1.24.6 Configuring Network Management Functions

1. Requirements

Configure network management functions on Device A to realize information management interaction from the NMS to the agent through SNMP. The NMS server IP address is 192.168.2.2.

2. Topology

Figure 1-19 Topology of Network Management Functions



3. Notes

- Bind MIB to the OSPF process on Device A.
- Configure the trap function on Device A.

4. Procedure

(1) Configure interface IP addresses for all devices (omitted).

(2) Configure OSPF basic functions on all devices (omitted).

(3) Bind MIB to the OSPF process on Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# snmp-server host 192.168.2.2 traps version 2c public
Device A(config)# snmp-server community public rw
Device A(config)# snmp-server enable traps
```

(4) Configure the trap function in OSPF process 10.

```
Device A(config)# router ospf 10
Device A(config-router)# enable mib-binding
Device A(config-router)# enable traps
```

5. Verification

Verify the SNMP information before the trap function is configured for the OSPF process.

```
Device A# show snmp
Chassis: 60FF60
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
```

```
  0 Get-next PDUs
  0 Set-request PDUs
  0 Drop PDUs
  0 UDP parse errors
0 SNMP packets output
  0 Too big errors (Maximum packet size 1472)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs
SNMP global trap: disabled
SNMP logging: disabled
SNMP trap logging: disabled
SNMP agent: enabled
SNMP v1:  enabled
SNMP v2c: enabled
SNMP v3:  enabled
```

Verify the SNMP information after the trap function is configured for the OSPF process.

```
Device A# show snmp
Chassis: 60FF60
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  8 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Drop PDUs
  0 UDP parse errors
2 SNMP packets output
  0 Too big errors (Maximum packet size 1472)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  2 Trap PDUs
```

6. Configuration Files

- Device A configuration file

```
!
snmp-server host 192.168.2.2 traps version 2c public
snmp-server community public rw
snmp-server enable traps
!
router ospf 10
enable mib-binding
enable traps
!
```

7. Common Errors

- Configurations on the SNMP server are incorrect. For example, the MIB or trap function is not enabled.

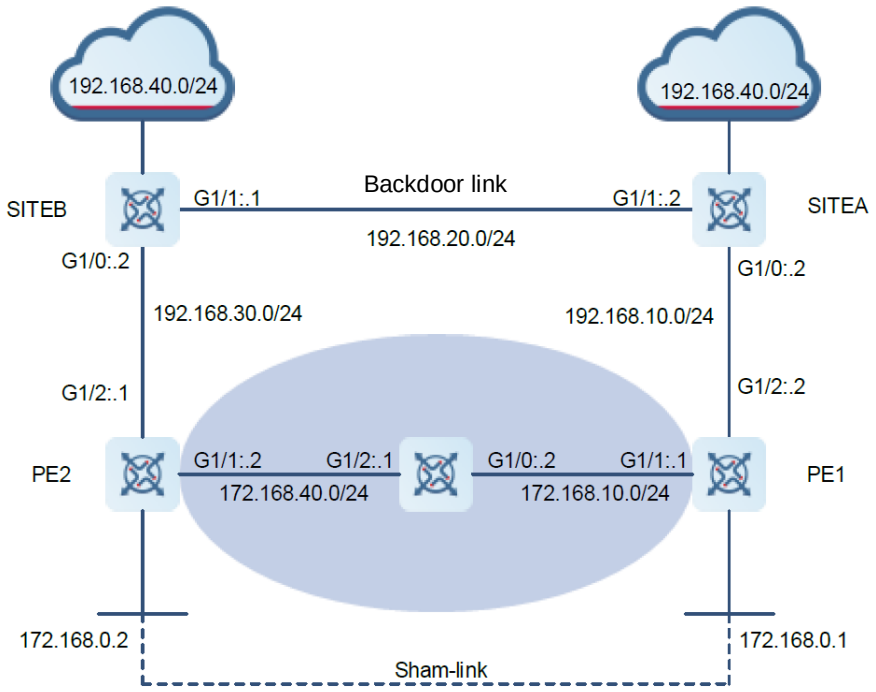
1.24.7 Configuring the Sham Link Function

1. Requirements

Two different sites of the client interact VPN routes through the MPLS backbone network. At the same time, a "backdoor link" is assumed between the two sites, and aims to ensure that, when the MPLS backbone network fails, information interaction between the two sites can be still implemented normally through this backup link.

2. Topology

Figure 1-20 Topology for Sham Link Function



3. Notes

- Configure on Site A to run the OSPF protocol with PE 1 and Site B, where the OSPF protocol runs with Site B through the backdoor link. Configure the OSPF cost for the interface.
- Configure on Site B to run the OSPF protocol with PE 2 and Site A, where the OSPF protocol runs with Site A through the backup link. Configure the OSPF cost for the interface.
- Configure a loopback interface on PE 1, create a VRF: VPN A, define the RD value and RT value, associate VRF with the corresponding interface, and associate the interface connecting to the CE with VRF; configure a loopback interface of VRF to establish a sham link, configure BGP, establish an MP-IBGP session with PE 2, implement route interaction with CE through the OSPF protocol, establish a sham link with the OSPF process on PE 2, configure MPLS signaling of the backbone network, enable the MPLS capability of public network interface, and configure the backbone network routing protocol.
- Configure a loopback interface on PE 2, create a VRF: VPN A, define the RD value and RT value, associate VRF with the corresponding interface, and associate the interface connecting to the CE with VRF; configure a loopback interface of VRF to establish a sham link, configure BGP, establish an MP-IBGP session with PE 1, implement VPN route interaction with CE through the OSPF protocol, and configure to establish a sham link with PE 1; configure MPLS signaling of the backbone network, enable the MPLS capability of public network interface, and configure the backbone network routing protocol.
- Configure backbone network MPLS signaling on P 1, enable the MPLS capability of interface, and configure the

backbone network routing protocol.

4. Procedure

(1) Make configuration on Site A.

Configure an IP address for the interface.

```
SITEA> enable
SITEA# configure terminal
SITEA(config)# interface GigabitEthernet 1/0
SITEA(config-GigabitEthernet 1/0)# ip address 192.168.10.2 255.255.255.0
SITEA(config-GigabitEthernet 1/0)# ip ospf cost 1
SITEA(config-GigabitEthernet 1/0)# exit
SITEA(config)# interface GigabitEthernet 1/1
SITEA(config-GigabitEthernet 1/1)# ip address 192.168.20.1 255.255.255.0
SITEA(config-GigabitEthernet 1/1)# ip ospf cost 200
SITEA(config-GigabitEthernet 1/1)# exit
```

Advertise the interface network to the OSPF process.

```
SITEA(config)# router ospf 10
SITEA(config-router)# network 192.168.10.0 255.255.255.0 area 0
SITEA(config-router)# network 192.168.20.0 255.255.255.0 area 0
```

(2) Make configuration on Site B.

Configure an IP address for the interface.

```
SITEB> enable
SITEB# configure terminal
SITEB(config)# interface GigabitEthernet 1/0
SITEB(config-GigabitEthernet 1/0)# ip address 192.168.30.2 255.255.255.0
SITEB(config-GigabitEthernet 1/0)# ip ospf cost 1
SITEB(config-GigabitEthernet 1/0)# exit
SITEB(config)# interface GigabitEthernet 1/1
SITEB(config-GigabitEthernet 1/1)# ip address 192.168.20.2 255.255.255.0
SITEB(config-GigabitEthernet 1/1)# ip ospf cost 200
SITEB(config-GigabitEthernet 1/1)# exit
```

Advertise the interface network to the OSPF process.

```
SITEB(config)# router ospf 10
SITEB(config-router)# network 192.168.30.0 255.255.255.0 area 0
SITEB(config-router)# network 192.168.20.0 255.255.255.0 area 0
```

(3) Make configuration on PE 1.

Configure loopback interface 0.

```
PE1> enable
PE1# configure terminal
```

```
PE1(config)# interface loopback 0
PE1(config-Loopback 0)# ip address 172.168.0.1 255.255.255.255
PE1(config-Loopback 0)# exit
```

Create a VRF VPNA and define its RD and RT attribute values.

```
PE1(config)# ip vrf VPNA
PE1(config-vrf)# rd 1:100
PE1(config-vrf)# route-target both 1:100
PE1(config-vrf)# exit
```

Configure an interface IP address and associate VRF with the corresponding interface.

```
PE1(config)# interface GigabitEthernet 1/2
PE1(config-GigabitEthernet 1/2)# ip vrf forwarding VPNA
PE1(config-GigabitEthernet 1/2)# ip address 192.168.10.1 255.255.255.0
PE1(config-GigabitEthernet 1/2)# exit
PE1(config)# interface loopback 10
PE1(config-Loopback 10)# ip vrf forwarding VPNA
PE1(config-Loopback 10)# ip address 192.168.0.1 255.255.255.255
PE1(config-Loopback 10)# exit
```

Configure BGP and establish an MP-IBGP session with PE 2.

```
PE1(config)# router bgp 1
PE1(config-router)# neighbor 172.168.0.2 remote-as 1
PE1(config-router)# neighbor 172.168.0.2 update-source loopback 0
PE1(config-router)# address-family vpnv4
PE1(config-router-af)# neighbor 172.168.0.2 activate
PE1(config-router-af)# exit
PE1(config-router)# exit
```

Configure to establish a sham link with the OSPF process on PE 2.

```
PE1(config)# router ospf 10 vrf VPNA
PE1(config-router)# network 192.168.10.0 255.255.255.0 area 0
PE1(config-router)# redistribute bgp subnets
PE1(config-router)# area 0 sham-link 192.168.0.1 192.168.0.2
PE1(config-router)# exit
```

Configure OSPF and direct route redistribution by BGP.

```
PE1(config)# router bgp 1
PE1(config-router)# address-family ipv4 vrf VPNA
PE1(config-router-af)# redistribute ospf 10
PE1(config-router-af)# redistribute connected
PE1(config-router-af)# exit
PE1(config-router)# exit
```

Configure backbone network MPLS signaling, and enable the MPLS capability of public network interface.

```
PE1(config)# mpls ip
```

```
PE1(config)# mpls router ldp
PE1(config-mpls-router)# ldp router-id interface loopback 0 force
PE1(config-mpls-router)# exit
PE1(config)# interface GigabitEthernet 1/1
PE1(config-GigabitEthernet 1/1)# ip address 172.168.10.1 255.255.255.0
PE1(config-GigabitEthernet 1/1)# label-switching
PE1(config-GigabitEthernet 1/1)# mpls ip
PE1(config-GigabitEthernet 1/1)# exit
```

Advertise the interface network to the OSPF process.

```
PE1(config)# router ospf 1
PE1(config-router)# network 172.168.10.0 0.0.0.255 area 0
PE1(config-router)# network 172.168.0.1 0.0.0.0 area 0
```

(4) Make configuration on PE 2

Configure loopback interface 0.

```
PE2> enable
PE2# configure terminal
PE2(config)# interface loopback 0
PE2(config-Loopback 0)# ip address 172.168.0.2 255.255.255.255
PE2(config-Loopback 0)# exit
```

Create a VRF VPNA and define its RD and RT attribute values.

```
PE2(config)# ip vrf VPNA
PE2(config-vrf)# rd 1:100
PE2(config-vrf)# route-target both 1:100
PE2(config-vrf)# exit
```

Configure an interface IP address and associate VRF with the corresponding interface.

```
PE2(config)# interface GigabitEthernet 1/2
PE2(config-GigabitEthernet 1/2)# ip vrf forwarding VPNA
PE2(config-GigabitEthernet 1/2)# ip address 192.168.30.1 255.255.255.0
PE2(config-GigabitEthernet 1/2)# exit
PE2(config)# interface loopback 10
PE2(config-Loopback 10)# ip vrf forwarding VPNA
PE2(config-Loopback 10)# ip address 192.168.0.2 255.255.255.255
PE2(config-Loopback 10)# exit
```

Configure BGP and establish an MP-IBGP session with PE 2.

```
PE2(config)# router bgp 1
PE2(config-router)# neighbor 172.168.0.1 remote-as 1
PE2(config-router)# neighbor 172.168.0.1 update-source loopback 0
PE2(config-router)# address-family vpnv4
PE2(config-router-af)# neighbor 172.168.0.1 activate
PE2(config-router-af)# exit
```

```
PE2(config-router)# exit
```

Configure to establish a sham link with the OSPF process on PE 2.

```
PE2(config)# router ospf 10 vrf VPNA
PE2(config-router)# network 192.168.30.0 255.255.255.0 area 0
PE2(config-router)# redistribute bgp subnets
PE2(config-router)# area 0 sham-link 192.168.0.2 192.168.0.1
PE2(config-router)# exit
```

Configure OSPF and direct route redistribution by BGP.

```
PE2(config)# router bgp 1
PE2(config-router)# address-family ipv4 vrf VPNA
PE2(config-router-af)# redistribute ospf 10
PE2(config-router-af)# redistribute connected
PE2(config-router-af)# exit
```

Configure backbone network MPLS signaling, and enable the MPLS capability of public network interface.

```
PE2(config)# mpls ip
PE2(config)# mpls router ldp
PE2(config-mpls-router)# ldp router-id interface loopback 0 force
PE2(config-mpls-router)# exit
PE2(config)# interface GigabitEthernet 1/1
PE2(config-GigabitEthernet 1/1)# ip address 172.168.40.2 255.255.255.0
PE2(config-GigabitEthernet 1/1)# label-switching
PE2(config-GigabitEthernet 1/1)# mpls ip
PE2(config-GigabitEthernet 1/1)# exit
```

Advertise the interface network to the OSPF process.

```
PE2(config)# router ospf 1
PE2(config-router)# network 172.168.40.0 0.0.0.255 area 0
PE2(config-router)# network 172.168.0.2 0.0.0.0 area 0
```

(5) Make configuration on P 1.

Configure loopback interface 0 on P 1.

```
P1> enable
P1# configure terminal
P1(config)# interface loopback 0
P1(config-Loopback 0)# ip address 172.168.0.3 255.255.255.255
P1(config-Loopback 0)# exit
```

Make basic configuration of OSPF.

```
P1(config)# router ospf 1
P1(config-router)# network 172.168.40.0 0.0.0.255 area 0
P1(config-router)# network 172.168.10.0 0.0.0.255 area 0
P1(config-router)# network 172.168.0.3 0.0.0.0 area 0
```

```
P1(config-router)# exit
```

Configure backbone network MPLS signaling on P 1, and enable the MPLS capability of interface.

```
P1(config)# interface GigabitEthernet 1/0
P1(config-GigabitEthernet 1/0)# ip address 172.168.10.2 255.255.255.0
P1(config-GigabitEthernet 1/0)# mpls ip
P1(config-GigabitEthernet 1/0)# label-switch
P1(config-GigabitEthernet 1/0)# exit
P1(config)# interface GigabitEthernet 1/1
P1(config-GigabitEthernet 1/1)# ip address 172.168.40.1 255.255.255.0
P1(config-GigabitEthernet 1/1)# mpls ip
P1(config-GigabitEthernet 1/1)# label-switch
P1(config-GigabitEthernet 1/1)# exit
P1(config)# mpls ip
P1(config)# mpls router ldp
PE2(config-mpls-router)# ldp router-id interface loopback 0 force
PE2(config-mpls-router)# exit
```

5. Verification

(1) Verify the configuration on PE 1.

Verify that an OSPF sham link route exists on PE 1.

```
PE1# show ip ospf 10 sham-links
Sham Link SLINK0 to address 192.168.0.2 is up
  Area 0.0.0.0 source address 192.168.0.1, Cost: 1
  Output interface is GigabitEthernet 1/1
  Nexthop address 172.16.40.2
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
    Adjacency state Full
```

Check the OSPF neighbor of PE 1.

```
PE1# show ip ospf 10 neighbor

OSPF process 10, 1 Neighbors, 1 is Full:
Neighbor ID    Pri   State             BFD State  Dead Time   Address
Interface
192.168.0.2       1   Full/ -            -        00:00:34   192.168.0.2
SLINK0
```

Check the VRF route of PE 1.

```
PE1# show ip route vrf VPNA
Routing Table: VPNA
```

```
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C      192.168.10.0/24 is directly connected, GigabitEthernet 1/2
O      192.168.20.0/24 [110/101] via 192.168.1.2, 00:56:23, GigabitEthernet 1/2
O      192.168.30.0/24 [110/2] via 172.168.0.2, 00:00:36
O      192.168.40.0/24 [110/2] via 172.168.0.2, 00:00:36
```

(2) Verify the configuration on PE 2.

Verify that an OSPF sham link route exists on PE 2.

```
PE2# show ip ospf 10 sham-links
Sham Link SLINK0 to address 192.168.0.1 is up
  Area 0.0.0.0 source address 192.168.0.2, Cost: 1
  Output interface is GigabitEthernet 1/1
  Nexthop address 172.16.10.1
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
    Adjacency state Full
```

Check the OSPF neighbor of PE 2.

```
PE2# show ip ospf 10 neighbor

OSPF process 10, 1 Neighbors, 1 is Full:
Neighbor ID    Pri   State             BFD State  Dead Time   Address
Interface
192.168.0.1       1   Full/ -            -        00:00:34   192.168.0.1
SLINK0
```

Check the VRF route of PE 2.

```
PE2# show ip route vrf VPNA
Routing Table: VPNA

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
```

```
Gateway of last resort is no set
O      192.168.10.0/24 [110/2] via 172.168.0.1, 00:00:36
O      192.168.20.0/24 [110/2] via 172.168.0.1, 00:00:36
C      192.168.30.0/24 is directly connected, GigabitEthernet 1/2
O      192.168.40.0/24 [110/101] via 192.168.30.2, 00:56:23, GigabitEthernet 1/2
```

6. Configuration Files

- Site A configuration file

```
!
interface GigabitEthernet 1/0
 ip address 192.168.10.2 255.255.255.0
 ip ospf cost 1
!
interface GigabitEthernet 1/1
 ip address 192.168.20.1 255.255.255.0
 ip ospf cost 200
!
router ospf 10
 network 192.168.10.0 255.255.255.0 area 0
 network 192.168.20.0 255.255.255.0 area 0
!
```

- Site B configuration file

```
!
interface GigabitEthernet 1/0
 ip address 192.168.30.2 255.255.255.0
 ip ospf cost 1
!
interface GigabitEthernet 1/1
 ip address 192.168.20.2 255.255.255.0
 ip ospf cost 200
!
router ospf 10
 network 192.168.30.0 255.255.255.0 area 0
 network 192.168.20.0 255.255.255.0 area 0
!
```

- PE 1 configuration file

```
!
ip vrf VPNA
 rd 1:100
 route-target both 1:100
```

```
!
interface GigabitEthernet 1/1
 ip address 172.168.10.1 255.255.255.0
 label-switching
 mpls ip
!
interface GigabitEthernet 1/2
 ip vrf forwarding VPNA
 ip address 192.168.10.1 255.255.255.0
interface loopback 0
 ip address 172.168.0.1 255.255.255.255
!
interface loopback 10
 ip vrf forwarding VPNA
 ip address 192.168.0.1 255.255.255.255
!
router bgp 1
 neighbor 172.168.0.2 remote-as 1
 neighbor 172.168.0.2 update-source loopback 0
 address-family vpnv4
  neighbor 172.168.0.2 activate
 address-family ipv4 vrf VPNA
  redistribute ospf 10
  redistribute connected
!
router ospf 1
 network 172.168.10.0 0.0.0.255 area 0
 network 172.168.0.1 0.0.0.0 area 0
!
router ospf 10 vrf VPNA
 network 192.168.10.0 255.255.255.0 area 0
 redistribute bgp subnets
 area 0 sham-link 192.168.0.1 192.168.0.2
!
mpls ip
mpls router ldp
 ldp router-id interface loopback 0 force
!
```

- PE 2 configuration file

```
!
ip vrf VPNA
 rd 1:100
```

```
 route-target both 1:100
!
interface GigabitEthernet 1/1
 ip address 172.168.40.2 255.255.255.0
 label-switching
 mpls ip
!
interface GigabitEthernet 1/2
 ip vrf forwarding VPNA
 ip address 192.168.30.1 255.255.255.0
!
interface loopback 0
 ip address 172.168.0.2 255.255.255.255
!
interface loopback 10
 ip vrf forwarding VPNA
 ip address 192.168.0.2 255.255.255.255
!
router bgp 1
 neighbor 172.168.0.1 remote-as 1
 neighbor 172.168.0.1 update-source loopback 0
 address-family vpnv4
  neighbor 172.168.0.1 activate
 address-family ipv4 vrf VPNA
  redistribute ospf 10
  redistribute connected
!
router ospf 1
 network 172.168.40.0 0.0.0.255 area 0
 network 172.168.0.2 0.0.0.0 area 0
!
router ospf 10 vrf VPNA
 network 192.168.30.0 255.255.255.0 area 0
 redistribute bgp subnets
 area 0 sham-link 192.168.0.2 192.168.0.1
!
mpls ip
mpls router ldp
 ldp router-id interface loopback 0 force
!
```

- P 1 configuration file

```
!
```

```
interface GigabitEthernet 1/0
 ip address 172.168.10.2 255.255.255.0
 mpls ip
 label-switch
!
interface GigabitEthernet 1/1
 ip address 172.168.40.1 255.255.255.0
 mpls ip
 label-switch
!
interface loopback 0
 ip address 172.168.0.3 255.255.255.255
!
router ospf 1
 network 172.168.40.0 0.0.0.255 area 0
 network 172.168.10.0 0.0.0.255 area 0
 network 172.168.0.3 0.0.0.0 area 0
!
mpls ip
mpls router ldp
 ldp router-id interface loopback 0 force
!
```

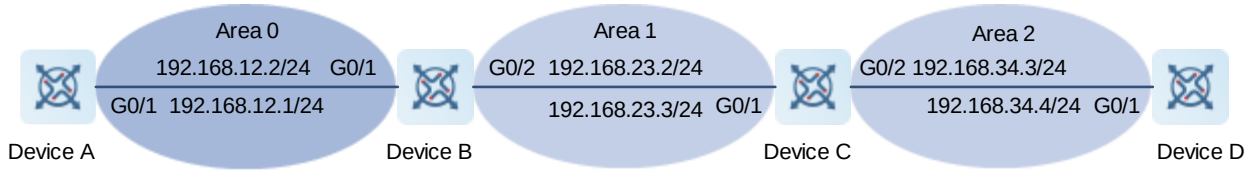
1.24.8 Configuring a Virtual Link

1. Requirements

Area 2 is not directly connected to Area 0. To ensure the normal operation of OSPF on the network, a virtual link is configured between Device B and Device C.

2. Topology

Figure 1-21 Topology for Configuring a Virtual Link



3. Notes

- Configure interface IP addresses for all devices (omitted).
- Configure OSPF basic functions on all devices (omitted).

- Configure a virtual link on Devices B and C.

4. Procedure

(1) Configure an IP address for each interface and the OSPF routing protocol (omitted).

(2) Configure a virtual link on Devices B and C.

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# router ospf 1
Device B(config-router)# area 1 virtual-link 192.168.23.3
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# router ospf 1
Device C(config-router)# area 1 virtual-link 192.168.12.2
```

5. Verification

Verify that the route of Area 2 can be learned by running the **show ip ospf database** command on Device A.

```
Device A# show ip ospf database
          OSPF Router with ID (192.168.12.1) (Process ID 1)
             Router Link States (Area 0)
Link ID        ADV Router     Age        Seq#      Checksum Link count
192.168.12.1   192.168.12.1   1025       0x80000002 0x00292E 1
192.168.12.2   192.168.12.2   3          0x80000004 0x00DA5E 2
192.168.23.3   192.168.23.3   7    (DNA) 0x80000001 0x001328 0
             Net Link States (Area 0)
Link ID        ADV Router     Age        Seq#      Checksum
192.168.12.2   192.168.12.2   1031       0x80000001 0x00CE8E
             Summary Net Link States (Area 0)
Link ID        ADV Router     Age        Seq#      Checksum
192.168.23.0   192.168.12.2   820        0x80000001 0x0077CC
192.168.23.0   192.168.23.3   7    (DNA) 0x80000001 0x002414
192.168.34.0   192.168.23.3   7    (DNA) 0x80000001 0x00AA82
```

6. Configuration Files

- Device B configuration file

```
!
router ospf 1
area 1 virtual-link 192.168.23.3
!
```

- Device C configuration file

```
!
router ospf 1
 area 1 virtual-link 192.168.12.2
!
```

1.24.9 Selecting a DR of OSPF

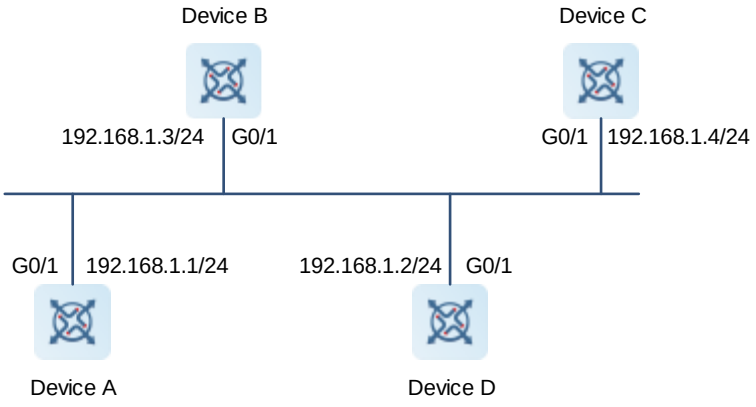
1. Requirements

Devices A, B, C, and D are on the same broadcast network.

Configure the priority of Device A as 10 to turn it into a DR, and the priority of Device B as 5 to turn it into a BDR, set the default priority for Device C, and set the priority of Device D to 0 to avoid participating in DR election.

2. Topology

Figure 1-22 Topology for Selecting a DR



3. Notes

Set the priorities to 10, 5, and 0 on Devices A, B, and D respectively.

4. Procedure

(1) Configure an IP address for each interface and the OSPF routing protocol (omitted).

(2) Set the priorities on Devices A, B, and D.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip ospf priority 10
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip ospf priority 5
```

Configure Device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# interface GigabitEthernet 0/1
Device D(config-if-GigabitEthernet 0/1)# ip ospf priority 0
```

5. Verification

Verify that the displayed neighbor is correct when the **show ip ospf neighbor** command is run on Device D.

```
Device D# show ip ospf neighbor
Neighbor ID     Pri   State          Dead Time   Address        Interface
192.168.1.1      10   FULL/DR       00:00:38    192.168.1.1    GigabitEthernet0/1
192.168.1.2      5   FULL/BDR       00:00:30    192.168.1.2    GigabitEthernet0/1
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
ip ospf priority 10
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
ip ospf priority 5
!
```

- Device D configuration file

```
!
interface GigabitEthernet 0/1
ip ospf priority 0
!
```

Contents

1 Configuring OSPFv3 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Basic Concepts 1
1.1.3 Principles 10
1.1.4 Protocols and Standards 18
1.2 Configuration Task Summary 18
1.3 Configuring Basic OSPFv3 Functions 19
1.3.1 Overview 19
1.3.2 Restrictions and Guidelines 19
1.3.3 Configuration Tasks 19
1.3.4 Configuring OSPFv3 19
1.3.5 Creating a Virtual Link 20
1.4 Configuring OSPFv3 Network Types 21
1.4.1 Overview 21
1.4.2 Restrictions and Guidelines 21
1.4.3 Prerequisites 21
1.4.4 Procedure 22
1.5 Configuring OSPFv3 Route Advertisement 22
1.5.1 Overview 22
1.5.2 Configuration Tasks 22
1.5.3 Configuring External Route Redistribution 23

1.5.4 Generating a Default Route 23

1.5.5 Configuring a Device as ASBR 24

1.5.6 Restrictions and Guidelines 24

1.6 Configuring Stub Area and NSSA 25

1.6.1 Overview 25

1.6.2 Restrictions and Guidelines 25

1.6.3 Prerequisites 25

1.6.4 Procedure 25

1.7 Configuring OSPFv3 Route Summarization 26

1.7.1 Overview 26

1.7.2 Restrictions and Guidelines 26

1.7.3 Prerequisites 26

1.7.4 Procedure 26

1.8 Configuring OSPFv3 Route Filtering 27

1.8.1 Overview 27

1.8.2 Restrictions and Guidelines 27

1.8.3 Prerequisites 27

1.8.4 Procedure 27

1.9 Adjusting OSPFv3 Routing 28

1.9.1 Overview 28

1.9.2 Restrictions and Guidelines 28

1.9.3 Prerequisites 29

1.9.4 Procedure 29

1.10 Adjusting OSPFv3 Network Convergence Speed 30

1.10.1 Overview 30

1.10.2 Prerequisites 30

1.10.3 Configuration Tasks 30

1.10.4 Configuring Transmission Time of OSPFv3 Packets 30

1.10.5 Configuring OSPFv3 Route Computation Time 31

1.11 Enabling OSPFv3 Authentication 33

1.11.1 Overview 33

1.11.2 Restrictions and Guidelines 33

1.11.3 Prerequisites 33

1.11.4 Configuration Tasks 33

1.11.5 Configuring Area Authentication and Encryption 33

1.11.6 Configuring Interface Authentication and Encryption 34

1.12 Enabling Two-Way Maintenance 35

1.12.1 Overview 35

1.12.2 Prerequisites 35

1.12.3 Procedure 35

1.13 Correlating OSPFv3 with BFD 36

1.13.1 Overview 36

1.13.2 Restrictions and Guidelines 36

1.13.3 Prerequisites 36

1.13.4 Procedure 36

1.14 Enabling the GR Function 37

1.14.1 Overview 37

1.14.2 Restrictions and Guidelines 37

1.14.3 Prerequisites 37

1.14.4 Procedure 37

1.15 Enabling NSR 37

1.15.1 Overview 37

1.15.2 Restrictions and Guidelines 38

1.15.3 Prerequisites 38

1.15.4 Procedure 38

1.16 Modifying the Maximum Number of Concurrent Neighbors 38

1.16.1 Overview 38

1.16.2 Procedure 38

1.17 Configuring Network Management Functions 39

1.17.1 Overview 39

1.17.2 Restrictions and Guidelines 39

1.17.3 Prerequisites 39

1.17.4 Procedure 39

1.18 Disabling MTU Verification 40

1.18.1 Overview 40

1.18.2 Prerequisites 40

1.18.3 Procedure 40

1.19 Enabling OSPFv3 on a Super VLAN 40

1.19.1 Overview 40

1.19.2 Restrictions and Guidelines 40

1.19.3 Prerequisites 41

1.19.4 Procedure 41

1.20 Monitoring 41

1.21 Configuration Examples 42

1.21.1 Configuring Basic Functions of OSPFv3 42

1.21.2 Configuring OSPFv3 Authentication 48

1.21.3 Configuring a Stub Area 49

1.21.4 Configuring an NSSA 51

1.21.5 Selecting an OSPFv3 DR 53

1.21.6 Configuring BFD for OSPFv3 56

1.21.7 Configuring OSPFv3 Route Summarization 60

1 Configuring OSPFv3

1.1 Introduction

1.1.1 Overview

The open shortest path first version 3 (OSPFv3) is an Interior Gateway Protocol (IGP) that is used within the autonomous system (AS) to allow routers to obtain a route to a remote network.

Note

- OSPFv2 is applicable to IPv4, and OSPFv3 is applicable to IPv6. The protocol running mechanism and most configurations are the same.

OSPFv3 has the following characteristics:

- Wide scope of application: OSPFv3 is applicable to a larger-scale network that supports hundreds of routers.
- Fast convergence: Once the network topology changes, advertisements can be quickly sent between routers to update routes.
- No self-loop: Only the link status information is synchronized between routers. Each router computes routes independently, and a self-loop will not occur.
- Area division: A large routing domain is divided into multiple small areas to save system resources and network bandwidth and ensure stability and reliability of routes.
- Route classification: Routes are classified into several types to support flexible control.
- Equivalent routes: OSPFv3 supports equivalent routes.
- Authentication: OSPFv3 supports packet authentication to ensure security of protocol interaction.
- Multicast transmission: Protocol packets are sent using the multicast address to avoid interfering with irrelevant entities and save system resources.

Note

- In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be layer-3 (L3) switches, routers, or firewalls.

1.1.2 Basic Concepts

1. Routing domain

All routers in an AS must be interconnected and use the same routing protocol. Therefore, an AS is also called a routing domain.

An AS in which OSPFv3 runs is also called OSPFv3 routing domain (short for OSPFv3 domain).

2. OSPFv3 process

OSPFv3 supports multiple instances, and each instance corresponds to an OSPFv3 process.

One or more OSPFv3 processes can be started on a router. Each OSPFv3 process runs OSPFv3 independently, and the processes are mutually isolated.

An OSPFv3 packet header contains the Instance ID field, and multiple OSPFv3 instances can run concurrently on a single link. The process ID is valid only on the local device.

3. Router ID

The router ID uniquely identifies a router in an OSPFv3 domain. Router IDs of any two routers cannot be the same.

If multiple OSPFv3 processes exist on a router, each OSPFv3 process uses one router ID. Router IDs of any two OSPFv3 processes cannot be the same.

4. OSPFv3 areas

OSPFv3 supports multiple areas. An OSPFv3 domain is divided into multiple areas to ease the computing pressure of a large-scale network.

An area is a logical group of routers, and each group is identified by an area ID. The border between areas is a router. A router may belong to one area or multiple areas. One network segment (link) can belong to only one area, or each OSPFv3 interface must belong to a specified area.

- Backbone area and normal area

  Area 0 is a backbone area, and other areas are normal areas. Normal areas must be directly connected to the backbone area.

- Stub area

  Configuring an OSPFv3 stub area can reduce the number of Link-State Advertisements (LSAs) in the area. The area border router (ABR) in the stub area will not transfer the Type 5 LSA (external route), and will advertise the default route to the stub area.

- Totally stub area

  A totally stub area is upgraded from a stub area. The router in the totally stub area will not transfer Type 3 LSA (inter-domain route) and Type 5 LSA (external route), and will advertise the default route to the stub area.

- NSSA

  A not-so-stubby area (NSSA) is similar to a stub area, but allows AS boundary routers (ASBRs). The route redistributed by an ASBR will be transferred in the NSSA in the form of Type 7 LSA, and the Type 7 LSA will be translated to Type 5 LSA on ABR and then transferred to other areas. The ABR also advertises the default route to the NSSA.

- Totally NSSA

  The relationship between the totally NSSA and NSSA is similar to that between the totally stub area and stub area. The totally NSSA forbids transfer of the Type 3 LSA (inter-domain route) on the basis of NSSA.

Caution

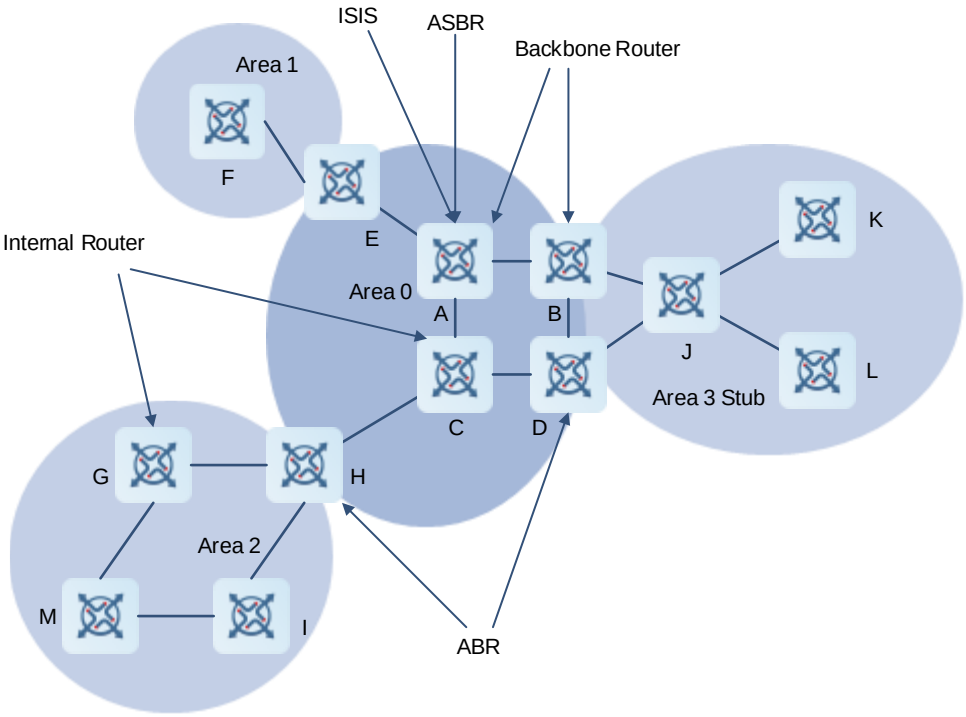
The backbone area cannot be a stub area, totally stub area, NSSA, or totally NSSA.

The stub area and totally stub area cannot contain any ASBR.

The stub area, totally stub area, NSSA, and totally NSSA cannot contain any virtual link.

The stub area, totally stub area, NSSA, and totally NSSA are special forms of normal areas and help reduce the load of routers and enhance reliability of OSPFv3 routes.

Figure 1-1 Classification of OSPFv3 Areas



5. OSPFv3 routers

The following types of routers are defined in OSPFv3 and assigned with different responsibilities:

- Internal router

  All interfaces of an internal router belong to the same OSPFv3 area, for example, A, C, F, G, I, M, J, K, and L shown in Figure 1-1.

- ABR

  An ABR is used to connect the backbone area with a normal area. An ABR belongs to two or more areas, and one of the areas must be the backbone area, for example, B, D, E, and H shown in Figure 1-1.

- Backbone router

  A backbone router has at least one interface that belongs to the backbone area. All ABRs and all routers in area 0 are backbone routers, for example, A, B, C, D, E, and H shown in Figure 1-1.

- ASBR

  An ASBR is used to exchange routing information with other ASs. An ASBR is not necessarily located on the border of an AS. It may be a router inside an area or an ABR, for example, A shown in Figure 1-1.

6. OSPFv3 Route Types

Each OSPFv3 route is marked to indicate the type of the route. There are six types of OSPFv3 routes:

- O: Internal route

This type of route describes how to arrive at a destination network in the local area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.

- OI: Inter-area route

  This type of route describes how to arrive at a destination network in another area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.

- OE1: Type 1 external route

  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.

- OE2: Type 2 external route

  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.

- ON1: Type 1 external route of the NSSA

  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA.

- ON2: Type 2 external route of the NSSA

  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA.

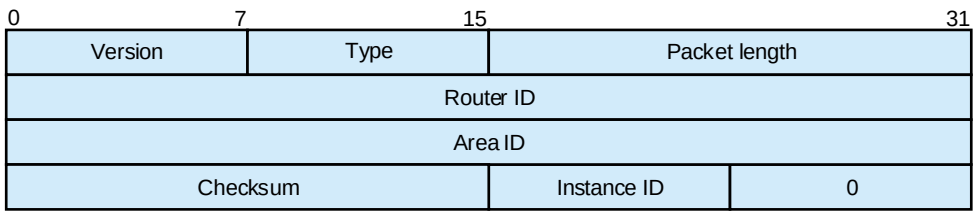
Note

Reliability of OE2 and ON2 routes is poor. OSPFv3 believes that the cost of the route from the ASBR to a destination network outside an AS is far greater than the cost of the route to the ASBR within the AS. Therefore, when the route cost is computed, only the cost of the route from the ASBR to a destination network outside an AS is considered.

7. OSPFv3 packets

The following table lists the OSPFv3 packets. These OSPFv3 packets are encapsulated in IP packets and transmitted in multicast or unicast mode.

Figure 1-2 OSPFv3 packet format



Version: indicates an OSPF version. The value is 3 for OSPFv3.

Type: indicates an OSPFv3 packet type.

Packet length: indicates the length of an OSPFv3 packet plus the packet head, in bytes.

Router ID: indicates the ID of a router that sends OSPFv3 packets.

Area ID: indicates the area of a router that sends OSPFv3 packets.

Checksum: indicates the checksum of an OSPFv3 packet, excluding the authentication field.

Instance ID: indicates an OSPFv3 instance ID.

0: reserved value.

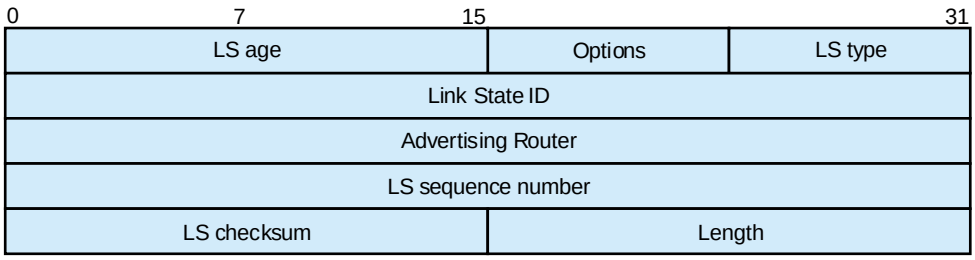
Table 1-1 Types of OSPFv3 Packets

Packet Type	Description
Hello	Hello messages are sent periodically to discover and maintain OSPFv3 neighbor relationships. The value of this OSPFv3 packet type is **1**.
Database description (DD)	DD packets carry brief information about the local link-state database (LSDB) and are used to synchronize databases between OSPFv3 neighbors. The value of this OSPFv3 packet type is **2**.
Link state request (LSR)	LSR packets are sent only after DD packets are exchanged successfully between OSPFv3 neighbors, and are used to request LSAs. The value of this OSPFv3 packet type is **3**.
Link state update (LSU)	LSU packets are used to send the required LSAs to peers. The value of this OSPFv3 packet type is **4**.
Link state acknowledgment (LSAck)	LSAck packets are used to acknowledge the received LSAs. The value of this OSPFv3 packet type is **5**.

8. LSA

OSPFv3 describes the routing information by means of LSAs.

Figure 1-3 LSA Packet Format



LS age: indicates the LS aging time of an LSA after it is generated, in seconds.

Option: is an optional field that decides whether to broadcast AS-external-LSAs, forward IP multicast packets, and process NSSA LSAs and on-demand links.

LS type: indicates different LSAs.

Link State ID: specifies a unique LSA in a routing domain together with the LSA type.

Advertising Router: indicates the ID of a router that generates this LSA.

LS sequence number: indicates the sequence number of an LSA, which is used to describe the generated sequence of LSAs.

LS checksum: indicates checksum of fields except the LS age field.

Length: indicates the total length of an LSA packet plus header, in bytes.

Table 1-2 Types of OSPFv3 LSAs

LSA Type	Description
Router-LSA (Type1)	This LSA is originated by every router. It describes the link state and cost of the router, and is advertised only within the area where the originating router is located.
Network-LSA (Type2)	This LSA is originated by a designated router (DR). It describes the state of the current link, and is advertised only within the area where the DR is located.
Inter-Area-Prefix-LSA (Type3)	This LSA is originated by an ABR. It describes a route to another area, and is advertised to areas except totally stub areas and NSSAs.
Inter-Area-Router-LSA (Type4)	This LSA is originated by an ABR. It describes a route to an ASBR, and is advertised to areas except the area where the ASBR is located.
AS-external-LSA (Type5)	This LSA is originated by an ASBR. It describes a route to a destination outside the AS, and is advertised to all areas except stub areas and NSSAs.
NSSA LSA (Type7)	This LSA is originated by an ASBR. It describes a route to a destination outside the AS, and is advertised only within the NSSA.
Link-LSA (Type8)	This LSA is originated by every router. It describes the link-local address and IPv6 prefix address of each link, and provides the link option that will be set in the Network-LSA. It is advertised only on the current link.
Intra-Area-Prefix-LSA (Type9)	Every router or DR generates one or more this type of LSAs, which are advertised in the area to which the router or DR belongs. The LSAs generated by a router describe the prefix of an IPv6 address associated with the Route-LSA. The LSAs generated by a DR describe the prefix of an IPv6 address associated with the Network-LSA.

9. OSPFv3 neighbor state

In the OSPFv3 network, neighbor devices need to reach the adjacency state before exchanging link information. There are several OSPFv3 neighbor states listed below. When a neighbor enters the full state, the adjacency relationship is established.

Table 1-3 OSPFv3 Neighbor State Machine and Description

State	Description
Down	The state of the first OSPFv3 neighbor, which indicates that the neighbor's hello packet is not received within the neighbor dead interval.
Attempt	The attempt state router sends a hello packet to the manually configured neighbor periodically. The attempt state applies to the interfaces of NBMA type only.
Init	A hello packet has been received from the neighbor, but the packet does not contain the router ID of the neighbor receiving router, that is, the peer end does not receive the hello packet sent by the local end.
Two-Way	Indicates mutual neighbors. When the neighbor router ID field in the received hello packet is each other's router ID, and both ends receive the hello packet sent from the peer end, a neighbor relationship is established. After this phase ends, DR and backup designated router (BDR) will be selected for broadcast and non-broadcast multi-access.
Exstart	Indicates negotiation about the master/slave relationship. The initial sequence number for forming an adjacency is selected, and the master/slave relationship ensures orderly transmission in the subsequent exchange of DD packets.
Exchange	Indicates exchange of DD packets. Checks whether the neighbor can provide new or updated link state information.
Loading	Indicates that, based on the information provided by DBD, the router will send LSR and interactive LSU to implement synchronization with LSDB.
Full	Indicates establishment of an adjacency. Indicates that the LSDBs of the two devices have been synchronized, and the adjacency state has been established between the local device and the neighbor device.

10. OSPFv3 network types

A router does not necessarily need to exchange LSAs with every neighbor or set up an adjacency with every neighbor. To improve efficiency, OSPFv3 classifies networks that use various link layer protocols into five types so that LSAs are exchanged in different ways to set up an adjacency.

By default, Ethernet and FDDI belong to the broadcast type, X.25, frame relay, and ATM belong to the NBMA type, and PPP, HDLC, and LAPB belong to the P2P type.

Table 1-4 Introduction to OSPFv3 Network Types

Network Type	Link Layer Protocol	Neighbor Relationship and DR Election
Broadcast	Ethernet and FDDI belong to the broadcast network type by default.	Neighbors are automatically discovered, and the DR and BDR are elected. The DR or BDR exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.
NBMA	X.25, frame relay, and ATM belong to NBMA networks by default.	Neighbors are manually configured, and the DR and BDR are elected. The DR or BDR exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.
Point-to-Point (P2P)	PPP, HDLC, and LAPB belong to the P2P network type by default.	Neighbors are automatically discovered, and the DR or BDR is not elected. LSAs are exchanged between routers at both ends of the link, and the adjacency is set up.
Point-to-Multipoint (P2MP)	Networks without any link layer protocol belong to the P2MP network type by default.	Neighbors are automatically discovered, and the DR or BDR is not elected. LSAs are exchanged between any two routers, and the adjacency is set up.
P2MP broadcast	Networks without any link layer protocol belong to the P2MP network type by default.	Neighbors are manually configured, and the DR or BDR is not elected. LSAs are exchanged between any two routers, and the adjacency is set up.

11. DR and BDR

In the broadcast or NBMA network, many unwanted LSAs will be created when an adjacency is set up with related routers. If there are n routers, n × (n-1)/2 adjacency relationships will be set up, and n^2 LSAs will be generated in the network. In the process of setting up the adjacency and exchanging LSAs, many unwanted copies will be produced, which leads to chaos in the flooding of a multi-access network. To avoid these problems on a multi-access network, OSPFv3 defines the concepts of DR and BDR.

After the DR and BDR are elected, all routers will set up an adjacency relationship with the DR and BDR only, send information to the DR/BDR, and the DR will broadcast the network link state. The routers other than DR and BDR are called DROther routers and they will no longer set up an adjacency relationship or exchange any routing information with each other, thus reducing the number of adjacency relationships between routers on the broadcast and NBMA networks.

Figure 1-4 Number of Adjacency Relationships Before DR Election

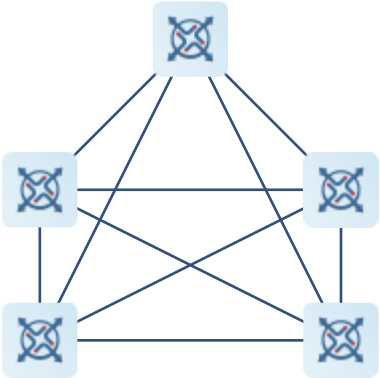
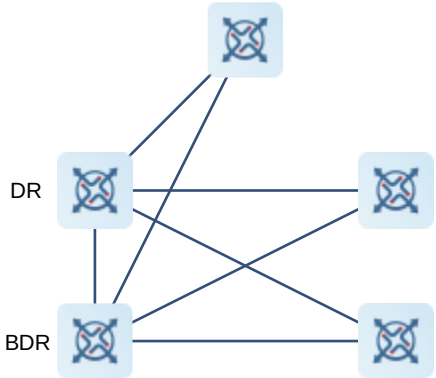


Figure 1-5 Number of Adjacency Relationships After DR Election

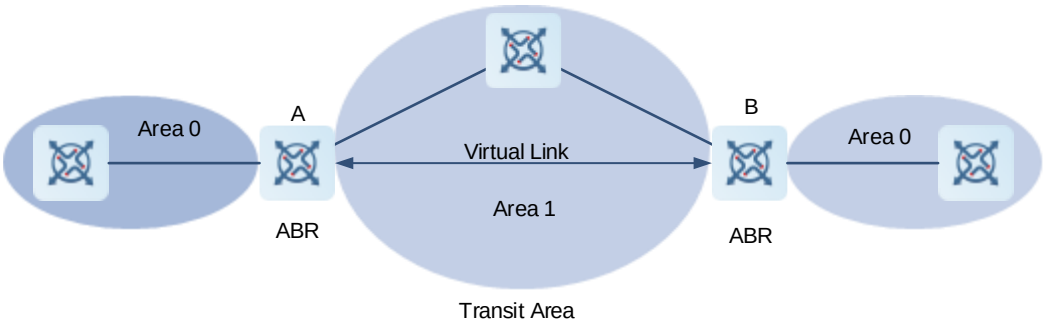


12. Virtual link

OSPFv3 supports virtual links. A virtual link is a logical link that belongs to the backbone area. It is used to resolve the problems such as a discontinuous backbone area or a failure to directly connect a normal area to the backbone area on the physical network. A virtual link supports traversal of only one normal area, and this area is called transit area. Routers on both ends of a virtual link are ABRs.

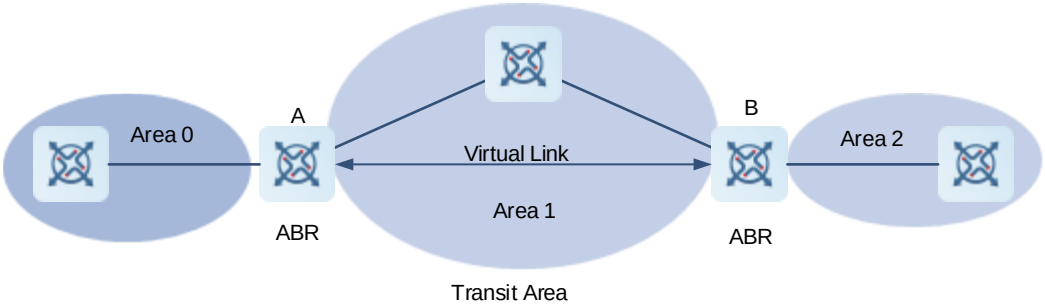
A virtual link relies on an OSPFv3 intra-domain route, making two ABRs adjacent. The OSPFv3 packet information exchanged by ABRs is transparent to the intermediate device.

Figure 1-6 Discontinuous Backbone Area on the Physical Network



As shown in Figure 1-6, a virtual link is set up between A and B to connect to Area 0. Area 1 is a transit area, and A and B are ABRs of Area 1.

Figure 1-7 Failure to Directly Connect a Normal Area to the Backbone Area on the Physical Network



As shown in Figure 1-7, a virtual link is set up between A and B to extend Area 0 to B so that Area 0 can be directly connected to Area 2 on B. Area 1 is a transit area, A is an ABR of Area 1, and B is an ABR of Area 1 and Area 2.

1.1.3 Principles

1. Simple principles

OSPFv3 is a type of link-state routing protocols. Its working process consists of three phases:

(1) Neighbor discovery > Bidirectional communication

An OSPFv3 neighbor relationship is set up between adjacent routers, and bidirectional communication is maintained.

(2) Database synchronization > Full adjacency

A router uses LSAs to advertise all its link states. LSAs are exchanged between neighbors and the LSDB is synchronized to achieve full adjacency.

(3) Shortest Path Tree (SPT) computation > Formation of a routing table

The router computes the shortest path to each destination network based on the LSDB and forms an OSPFv3 routing table.

- Neighbor discovery > Bidirectional communication

  Routers send hello packets through all OSPFv3-enabled interfaces or virtual links. If hello packets can be exchanged between two routers, and parameters carried in the hello packets can be successfully

negotiated, the two routers become neighbors. When routers that are mutual neighbors find their own router IDs from hello packets sent from neighbors, bidirectional communication is set up.

A hello packet includes, but is not limited to, the following information:

- ID of the originating router
- Area ID of the originating router interface or virtual link
- Instance ID of the originating router interface or virtual link
- Interface ID of the originating router interface or virtual link
- Priority of the originating router interface (used for DR/BDR election)
- Hello interval of the originating router interface or virtual link
- Neighbor dead interval of the originating router interface or virtual link
- IDs of the DR and BDR
- Router ID of the neighbor of the originating router

- Database synchronization > Full adjacency

  After bidirectional communication is set up between neighbor routers, the DD, LSR, LSU, and LSAck packets are used to exchange LSAs and set up the adjacency. The brief process is as follows:

  - A router generates an LSA to describe all link states on the router.
  - The LSA is exchanged between neighbors. When a router receives the LSA from its neighbor, it copies the LSA and saves the copy in the local LSDB, and then advertises the LSA to other neighbors.
  - When the router and its neighbors obtain the same LSDB, full adjacency is achieved.

Note

OSPFv3 will be very stable without change in link cost or network addition or deletion. If any change takes place, the changed link states are advertised to quickly synchronize the LSDB.

- SPT computation > Formation of a routing table

  After the complete LSDB is obtained from the router, the Dijkstra algorithm is run to generate an SPT from the local router to each destination network. The SPT records the destination networks, next-hop addresses, and cost. OSPFv3 generates a routing table based on the SPTs.

  If change in link cost or network addition or deletion takes place, the LSDB will be updated. The router again runs the Dijkstra algorithm, generates a new SPT, and updates the routing table.

Note

The Dijkstra algorithm is used to find the shortest path from a vertex to other vertices in a weighted directed graph.

2. OSPFv3 routing

- Routing cost

  If redundancy links or devices exist in the network, multiple paths may exist from the local device to the destination network. OSPFv3 selects the path with the minimum total cost to form an OSPFv3 route. The

total cost of a path is equal to the sum of the costs of individual links along the path. The total cost of a path can be minimized by modifying the costs of individual links along the path. In this way, OSPFv3 selects this path to form a route.

With configuration commands, you can modify the following link costs:

- Cost from the interface to the directly-connected network segment
- Cost from the interface to the neighbor (from local device to a specified neighbor)
- Cost from the ABR to the default network segment (cost of the default route that the ABR automatically advertises to the stub area and NSSA)
- Cost from the ASBR to an external network segment (cost of the default route that the ABR automatically advertises to the stub area and NSSA)
- Cost from the ASBR to the default network segment (cost of the default route that is manually introduced)

- OSPFv3 administrative distance

  The administrative distance (AD) is used to evaluate the reliability of various route sources. Its value is an integer ranging from 0 to 255. A smaller AD value indicates that the route is more trustworthy. If there are multiple routes to the same destination, the router preferentially selects a route with a smaller AD value. The route with a greater AD value becomes a floating route, that is, a standby route of the optimum route.

  By default, the route coming from one source corresponds to an AD value. The AD value is a local concept. Modifying the AD value affects route selection only on the current router.

Table 1-5 Routing Protocols and Default Administrative Distances

Route Source	Directly-connected network	Static route	EBGP route	OSPFv3 route	IS-IS route	RIP route	IBGP route	Unreachable route
Default AD	0	1	20	110	115	120	200	255

3. OSPFv3 route advertisement

- Route redistribution

  Route redistribution refers to the process of introducing routes of other routing protocols, routes of other OSPFv3 processes, static routes, and direct routes that exist on the device to an OSPFv3 process so that these routes can be advertised to neighbors using Type 5 and Type 7 LSAs. A default route cannot be introduced during route redistribution.

  Route redistribution is often used for interworking between ASs. You can configure route redistribution on an ASBR to advertise routes outside an AS to the interior of the AS, or routes inside an AS to the exterior of the AS.

- Default route introduction

  By configuring a command on an ASBR, you can introduce a default route to an OSPFv3 process so that the route can be advertised to neighbors using Type 5 and Type 7 LSAs.

Default route introduction is often used for interworking between ASs. One default route is used to replace all the routes outside an AS.

After configuration of route redistribution and introduction of a default route, the router automatically becomes an ASBR.

4. OSPFv3 route summarization

Route summarization is a process of summarizing routing information with the same prefix into one route, and advertising the summarized route (replacing a large number of individual routes) to neighbors. Route summarization helps reduce the protocol interaction load and the size of the routing table.

By default, the ABR advertises inter-area routing information by using Type 3 LSAs within a network segment, and advertises redistributed routing information by using Type 5 and Type 7 LSAs. If continuous network segments exist, you are advised to configure route summarization.

After route summarization is configured, the ABR sends only Type 3 LSAs that summarize prefix of IPv6 addresses, and the ASBR sends only Type 5 and Type 7 LSAs that summarize prefix of IPv6 addresses and will not send LSAs with the prefix of IPv6 addresses.

5. OSPFv3 route filtering

OSPFv3 allows filtering the learned and exchanged routes and LSAs so as to meet the security requirements in specific scenarios, for example, the routes of some network segments are not intended to be learned by other areas.

With configuration commands, you can configure route filtering for the following items:

- Interface: The interface is prevented from sending routing information (any LSA) or exchanging routing information (any LSA) with neighbors.
- Routing information outside an AS: Only the routing information that meets the filtering conditions can be redistributed to the OSPFv3 process (Type 5 and Type 7 LSAs).
- LSAs received by a router: In the OSPFv3 routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

6. Stub area and NSSA

The stub/totally stub area and NSSA/totally NSSA help reduce the protocol interaction load and the size of the routing table.

- If an appropriate area is configured as a stub/totally stub area or NSSA/totally NSSA, advertisement of a large number of Type 5 and Type 3 LSAs can be avoided within the area.

Table 1-6 LSAs in Stub Area/NSSA

Area	LSA Types 1 and 2	LSA Type 3	LSA Type 4	LSA Type 5	LSA Type 7
Non-stub/totally stub area and non-NSSA/totally NSSA	Allowed	Allowed	Allowed	Allowed	Not allowed

Area	LSA Types 1 and 2	LSA Type 3	LSA Type 4	LSA Type 5	LSA Type 7
Stub area	Allowed	Allowed (containing one default route)	Not allowed	Not allowed	Not allowed
Totally stub area	Allowed	Only one default route is allowed.	Not allowed	Not allowed	Not allowed
NSSA	Allowed	Allowed (containing one default route)	Allowed	Not allowed	Allowed
Totally NSSA	Allowed	Only one default route is allowed.	Allowed	Not allowed	Allowed

Note

- The ABR uses Type 3 LSAs to advertise a default route to the stub/totally stub area or NSSA/totally NSSA.
- The ABR translates Type 7 LSAs in the NSSA and totally NSSA to Type 5 LSAs, and advertises Type 5 LSAs to the backbone area.

- If an appropriate area is configured as a stub/totally stub area or NSSA/totally NSSA, a large number of OE1, OE2, and OI routes will not be added to the routing table of a router in the area.

Table 1-7 Route Types in Stub Areas/NSSAs

Area	Routes Available in the Routing Table of a Router Inside the Area
Non-stub/totally stub area and non-NSSA/totally NSSA	O: a route to a destination network in the local area OI: a route to a destination network segment in another area OE1 or OE2: a route or default route to a destination network segment outside the AS (via any ASBR in the AS)
Stub area	O: a route to a destination network in the local area OI: a route or a default route to a destination network segment in another area
Totally stub area	O: a route to a destination network in the local area OI: a default route

Area	Routes Available in the Routing Table of a Router Inside the Area
NSSA	O: a route to a destination network in the local area OI: a route or a default route to a destination network segment in another area ON1 or ON2: a route or default route to a destination network segment outside the AS (via an ASBR in the local area)
Totally NSSA	O: a route to a destination network in the local area OI: a default route ON1 or ON2: a route or default route to a destination network segment outside the AS (via an ASBR in the local area)

Note

- A backbone area cannot be configured as a stub area or an NSSA.
- A transit area with virtual links going through cannot be configured as a stub area or an NSSA.
- An area containing an ASBR cannot be configured as a stub area.

7. Enhanced security and reliability

The functions such as authentication and bidirectional forwarding detection (BFD) correlation are used to enhance security, stability, and reliability of OSPFv3.

- Authentication

  OSPFv3 uses IPv6 to provide two authentication mechanisms: authentication header (AH) and encapsulating security payload (ESP), to prevent illegal routers from accessing the network and prevent hosts that forge OSPFv3 packets from participating in OSPFv3 route switching. OSPFv3 packets received on the OSPFv3 interface or at both ends of a virtual link are authenticated. If authentication fails, the packets are discarded and no adjacency can be set up. Enabling authentication can avoid learning unauthenticated or invalid routes, thus preventing advertising valid routes to unauthenticated devices. In the broadcast-type network, authentication also prevents unauthenticated devices from becoming designated devices, ensuring stability of the routing system and protecting the routing system against intrusions.

  Authentication is classified into following two types:

  - Area authentication: This area-level authentication authenticates the packets transmitted by all the interfaces in the area. This authentication type is configured in OSPFv3 routing process mode.
  - Interface authentication: This neighbor-level authentication authenticates the packets transmitted on the related interface. This authentication type is configured in interface mode.

- MTU verification

  Upon receiving a DD packet, OSPFv3 checks whether the MTU of the neighbor interface is the same as that of the local interface. If the MTU of the interface specified in the received DD packet is greater than that

of the interface that receives the packet, the adjacency cannot be set up. Disabling MTU verification can avoid this problem.

- Two-way maintenance

  OSPFv3 routers periodically send hello packets to each other to maintain the adjacency. In a large network, a lot of packets may be sent or received, occupying a great proportion of CPU and memory. As a result, some packets are delayed or discarded. If the processing time of hello packets exceeds the dead interval, the adjacency will be destroyed.

  If the two-way maintenance function is enabled, in addition to the hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors, which makes the adjacency more stable.

- Concurrent neighbor interaction restriction

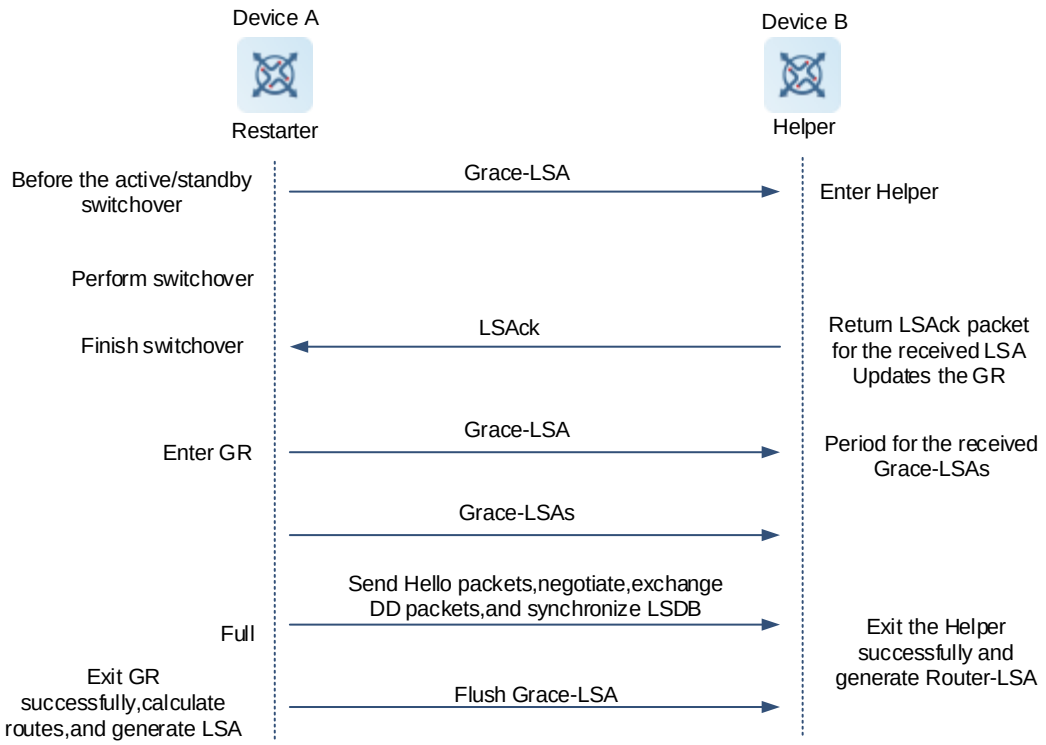
  When a router simultaneously exchanges data with multiple neighbors, its performance may be affected. If the maximum number of neighbors that concurrently initiate or accept interaction with the OSPFv3 process is restricted, the router can interact with neighbors by batches, which ensures data forwarding and other key services.

- GR

  The control and forwarding separated technology is widely used among routers. On a relatively stable network topology, when a graceful restart (GR) enabled router is restarted on the control plane, data forwarding can continue on the forwarding plane. In addition, actions (such as adjacency re-forming and route computation) performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

  Currently, the GR function is used only during active/standby switchover and system upgrade.

Figure 1-8 Normal OSPFv3 GR Process



- The GR process requires collaboration between the restarter and the helper. The restarter is the router where GR occurs. The helper is a neighbor of the restarter.
- When entering or exiting the GR process, the restarter sends a grace-LSA to the neighbor, notifying the neighbor to enter or exit the helper state.
- When the adjacency between the restarter and the helper reaches the full state, the router can exit the GR process successfully.

- **Fast hello**
  - Correlation with BFD

    After a link fails, it takes a period of time (about 40s) before OSPFv3 can sense the failure of the neighbor. Then, OSPFv3 advertises the information and re-computes the SPT. During this period, traffic is interrupted.
  - After the fast hello function is enabled (that is, the neighbor dead interval is set to 1s), OSPFv3 can sense the failure of the neighbor within 1s once a link is faulty. This accelerates route convergence and prevents traffic interruption.
  - BFD is used to test connectivity between devices. A link fault can be detected in as short as 150 ms. After OSPFv3 is correlated with BFD, OSPFv3 can sense the failure of a neighbor in as short as 150 ms once a link is faulty. This accelerates route convergence and prevents traffic interruption.

8. Network management functions

Functions such as management information base (MIB) and Syslog are used to facilitate OSPFv3 management.

- MIB

MIB is the device state information set maintained by a device. You can use the management program to view and set the MIB node.

Multiple OSPFv3 processes can be simultaneously started on a router, but the OSPFv3 MIB can be bound to only one OSPFv3 process.

- Trap

  A trap message is a notification generated when the system detects a fault. This message contains the related fault information.

  If the trap function is enabled, the router can actively send the trap messages to the network management device.

- Syslog

  The syslog records the operations (such as command configuration) performed by users on routers and specific events (such as network connection failures).

  If the syslog is allowed to record the adjacency changes, the network administrator can view the logs to learn the entire process from OSPFv3 adjacency setup to maintenance.

1.1.4 Protocols and Standards

- RFC 2740: This document describes the modifications to OSPFv3 to support version 6 of the Internet Protocol (IPv6).
- draft-ietf-ospf-ospfv3-graceful-restart: This document describes the OSPFv3 graceful restart. The OSPFv3 graceful restart is identical to OSPFv3v2 except for the differences described in this document. These differences include the format of the grace Link State Advertisements (LSA) and other considerations.
- draft-ietf-ospf-ospfv3-mib-11: This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in IPv6-based Internet. In particular, it defines objects for managing the Open Shortest Path First Routing Protocol for IPv6.

1.2 Configuration Task Summary

OSPFv3 configuration includes the following tasks:

(1) Configuring Basic OSPFv3 Functions

  a Configuring OSPFv3

  b (Optional) Creating a Virtual Link

(2) (Optional) Configuring OSPFv3 Network Types

(3) (Optional) Configuring OSPFv3 Route Advertisement. The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

  - Configuring External Route Redistribution
  - Generating a Default Route
  - Configuring a Device as ASBR

(4) (Optional) Configuring Stub Area and NSSA

(5) (Optional) Configuring OSPFv3 Route Summarization

(6) (Optional) Configuring OSPFv3 Route Filtering

(7) (Optional) Adjusting OSPFv3 Routing

(8) (Optional) Adjusting OSPFv3 Network Convergence Speed. The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring Transmission Time of OSPFv3 Packets
- Configuring OSPFv3 Route Computation Time

(9) (Optional) Enabling OSPFv3 Authentication. The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring Area Authentication and Encryption
- Configuring Interface Authentication and Encryption

(10) (Optional) Enabling Two-Way Maintenance

(11) (Optional) Correlating OSPFv3 with BFD

(12) (Optional) Enabling the GR Function

(13) (Optional) Enabling NSR

(14) (Optional) Modifying the Maximum Number of Concurrent Neighbors

(15) (Optional) Configuring Network Management Functions

(16) (Optional) Disabling MTU Verification

(17) (Optional) Enabling OSPFv3 on a Super VLAN

1.3 Configuring Basic OSPFv3 Functions

1.3.1 Overview

Set up an OSPFv3 routing domain in the network to provide IPv6 unicast routing service for users in the network.

1.3.2 Restrictions and Guidelines

- Ensure that the IPv6 routing function is enabled, that is, the **ipv6 routing** command is not disabled; otherwise, OSPFv3 cannot be enabled.
- The interface is configured with an IPv6 address.

1.3.3 Configuration Tasks

Basic OSPFv3 function configuration includes the following tasks:

(1) Configuring OSPFv3

(2) (Optional) Creating a Virtual Link

1.3.4 Configuring OSPFv3

1. Overview

The basic OSPFv3 functions are the prerequisites of all OSPFv3 functions. An OSPFv3 process must be created, a router ID can be specified for this process, and OSPFv3 must be configured on the interface.

2. Restrictions and Guidelines

- The configuration is mandatory for every OSPFv3 router.
- You are advised to configure the router ID.
- Run the **ipv6 ospf area** command in interface configuration mode to enable the OSPFv3 function on the interface, and then run the **ipv6 router ospf** command to configure an OSPFv3 process. After the OSPFv3 process is configured, the interface will automatically participate in the related process. The adjacency can be set up only between devices with the same instance ID.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an OSPFv3 process and enter OSPFv3 configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) (Optional) Configure a router ID.

router-id *router-id*

By default, the OSPFv3 routing process elects the largest IPv4 address among all the loopback interfaces as the router ID. If the loopback interfaces configured with IP addresses are not available, the OSPFv3 process elects the largest one among the IP addresses of all its physical interfaces as the router ID.

(5) Return to the global configuration mode.

exit

(6) Enter the interface configuration mode.

interface *interface-type interface-number*

(7) Enable OSPFv3 on the interface and specify an area ID.

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

OSPFv3 is disabled on an interface by default.

1.3.5 Creating a Virtual Link

1. Overview

In an OSPFv3 AS, all areas must be connected to the backbone area to properly learn the routing information of the entire OSPFv3 AS. If an area cannot be directly connected to the backbone area, the virtual link can be used to connect this area to the backbone area.

2. Restrictions and Guidelines

- The area where the virtual link is located cannot be a stub area or NSSA.
- At both ends of neighbors between which the virtual link is set up, settings of **hello-interval**, **dead-interval**, and **instance** must be consistent; otherwise, the adjacency cannot be set up properly.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Configure a virtual link.

area *area-id* **virtual-link** *router-id* [**dead-interval** *dead-interval* | **hello-interval** *hello-interval* | **instance** *instance-id* | **retransmit-interval** *retransmit-interval* | **transmit-delay** *transmit-delay*] * [**authentication ipsec spi** *spi* { **md**5 | **sha**1 } [0 | 7] *key* | **encryption ipsec spi** *spi* **esp** [3**des** | **aes-cbc** { 128 | 192 | 256 } [0 | 7] *des-key* | des [0 | 7] *des-key* | **null**] { **md**5 | **sha**1 } [0 | 7] *key*]

No virtual link is configured by default.

1.4 Configuring OSPFv3 Network Types

1.4.1 Overview

If the physical network is X.25, frame relay, or ATM, OSPFv3 can also run to provide the IPv6 unicast routing service.

OSPFv3 classifies networks into five types according to the link layer protocol type so that LSAs are exchanged in different ways to set up an adjacency. You can configure to forcibly change the network type of an interface.

1.4.2 Restrictions and Guidelines

- The broadcast network sends OSPFv3 multicast packets, automatically discovers neighbors, and elects a DR and a BDR.
- The P2P network sends OSPFv3 multicast packets and automatically discovers neighbors.
- The NBMA network sends OSPFv3 unicast packets. Neighbors must be manually specified, and a DR and a BDR must be elected.
- The P2MP network (without carrying the **non-broadcast** parameter) sends OSPFv3 multicast packets and automatically discovers neighbors.
- The P2MP network (carrying the **non-broadcast** parameter) sends OSPFv3 unicast packets. Neighbors must be manually specified.
- On a broadcast network, a DR or BDR must be elected. During the DR/BDR election, the device with a higher priority will be preferentially elected as a DR or BDR. If the priority is the same, the device with a larger router ID will be preferentially elected as a DR or BDR. A device with the priority 0 does not participate in the DR or BDR election.

1.4.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.4.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a network type for the interface.

ipv6 ospf network { **broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point** } [**instance** *instance-id*]

No interface type of OSPFv3 is configured by default. Routers at both ends of a link must be configured with the same network type.

(5) (Optional) Configure neighbors.

ipv6 ospf neighbor *ipv6-address* [**cost** *cost* | [**poll-interval** *poll-interval* | **priority** *value*] *] [**instance** *instance-id*]

No neighbor is configured by default.

(6) (Optional) Configure the interface priority.

ipv6 ospf priority *priority* [**instance** *instance-id*]

The priority value is 1 by default.

1.5 Configuring OSPFv3 Route Advertisement

1.5.1 Overview

The function aims to introduce unicast routes for other AS domains or default routes to other AS domains to the OSPFv3 domain and provides the unicast routing service to other AS domains for users in the OSPFv3 domain. The router that introduces routes will automatically become an ASBR.

OSPFv3 has two types of external routes. The metric of the Type 1 external route changes, but the metric of the Type 2 external route is fixed. If two parallel paths to the same destination network have the same route metric, the priority of Type 1 route is higher than that of Type 2 route. Therefore, running the **show ipv6 route** command displays only the Type 1 route.

1.5.2 Configuration Tasks

The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring External Route Redistribution
- Generating a Default Route
- Configuring a Device as ASBR

1.5.3 Configuring External Route Redistribution

1. Overview

Configure external route redistribution if external routes of the OSPFv3 domain need to be introduced to an ASBR.

2. Restrictions and Guidelines

- Configure **redistribute** on an ASBR.
- During redistribution of IS-IS routes, **level-1**, **level-2**, or **level-1-2** parameters can be configured to indicate that IS-IS routes of the specified levels are configured. By default, level-2 IS-IS routes are redistributed.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Configure external route redistribution.

redistribute { **bgp** | **connected** | **isis** [*area-tag*] [**level-1** | **level-1-2** | **level-2**] * | **ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **rip** | **static** } [**metric** *metric-value* | **metric-type** { **1** | **2** } | **route-map** *route-map-name* | **tag** *tag-value*] *

The route redistribution function is not enabled by default. The default metric type is **2**.

Level-2 routes are redistributed by default during IS-IS redistribution.

OSPFv3 routes of all sub-types are redistributed by default during OSPFv3 redistribution. The **route map** is not associated by default.

1.5.4 Generating a Default Route

1. Overview

A default route needs to be introduced to an ASBR so that other routers in the OSPFv3 domain access other AS domains through this ASBR by default.

2. Restrictions and Guidelines

- When the **redistribute** or **default-information** command is executed, the OSPFv3 router automatically becomes an ASBR.
- The ASBR, however, does not automatically generate or advertise a default route to all routers in the OSPFv3 routing domain. To enable an ASBR to generate a default route, run the **default-information originate** command.
- If the **always** parameter is specified, the OSPFv3 process advertises an external default route to neighbors no matter whether a default route exists in the core routing table. This default route, however, is not displayed on the local router. To confirm whether the default route is generated, run the **show ipv6 ospf**

database command to display the OSPFv3 link status database. On an OSPFv3 neighbor, you can run the **show ipv6 route ospf** command to see the default route.

- The metric of the external default route can be defined only by the **default-information originate** command, instead of the **default-metric** command.
- A router in a stub area cannot generate an external default route.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Generate a default route.

default-information originate [**always** | **metric** *metric* | **metric-type** *type* | **route-map** *map*] *

No default route is generated by default.

1.5.5 Configuring a Device as ASBR

1. Overview

Configure a device as ASBR in the AS domain or AS boundary.

1.5.6 Restrictions and Guidelines

After the **redistribute** or **default-information** command is executed, an OSPFv3 router automatically becomes an ASBR. If you want the device to become an ASBR without configuring the above command, run the **asbr enable** command.

If the **asbr enable** command is deleted, but the **redistribute** or **default-information** command configuration remains valid, the device is still an ASBR.

1. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Configure a device as ASBR.

asbr enable

No device is an ASBR by default.

1.6 Configuring Stub Area and NSSA

1.6.1 Overview

The function is used to configure an area located on the stub as a stub area to reduce interaction of routing information and the size of routing table, and enhance stability of routes. Devices in a stub area cannot learn the external routes (Type 5 LSAs) of the AS. In practice, external routes take up a large proportion of the LSDB. Therefore, devices in a stub area can learn only a small amount of routing information, which reduces the amount of system resources required to run the OSPFv3 protocol.

To reduce the size of the routing table on routers in the area and introduce OSPFv3 external routes to the area, configure the stub area as an NSSA.

1.6.2 Restrictions and Guidelines

- A backbone or transit area cannot be configured as a stub area or an NSSA.
- A router in the stub area cannot introduce external routes, but a router in the NSSA can introduce external routes.
- An area located on the stub of a network can be configured as a stub area. You must run the **area stub** command on all routers in a stub area.
- To configure a totally stub area, add the **no-summary** keyword when you are running the **area stub** command on the ABR.
- To configure a totally NSSA, you can configure the **no-summary** parameter on the ABR to prevent the ABR from sending the summary LSAs (Type 3 LSAs) to the NSSA.

1.6.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.6.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Configure a special OSPFv3 area. Configure one of the following tasks.

- Configure a stub area.

  area *area-id* **stub** [**no-summary**]

  The stub area function is disabled by default.

- Configure an NSSA.

  area *area-id* **nssa** [**default-information-originate** [**metric** *metric* | **metric-type** *metric-type*] * | **no-redistribution** | **no-summary** | **translator** [**always** | **stability-interval** ***stability-interval***] *] *

  The NSSA function is disabled by default.

1.7 Configuring OSPFv3 Route Summarization

1.7.1 Overview

Summarize routes to reduce interaction of routing information and the size of routing table, and enhance stability of routes.

Route summarization is classified into two types:

- Inter-area route summarization means to summarize routes between OSPFv3 areas.
- External route summarization means to summarize external routes of an OSPFv3 routing domain.

1.7.2 Restrictions and Guidelines

- The address range of the routes to be summarized may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table to shield or filter routes.
- Inter-area route summarization is configured and only takes effect on an ABR.
- External route summarization is configured on the ASBR that introduces routes.
- When configured on the NSSA ABR translator, **summary-prefix** summarizes redistributed routes and routes obtained based on the LSAs that are translated from Type 7 to Type 5. When configured on the ASBR (not an NSSA ABR translator), **summary-prefix** summarizes only redistributed routes.

1.7.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.7.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) (Optional) Configure inter-area route summarization.

area *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise** | **not-advertise**]

Inter-area route summarization is not performed by default.

(5) (Optional) Configure external route summarization.

summary-prefix *ipv6-prefix*/*prefix-length* [[**cost** *cost* | **tag** *tag-value*] * | **not-advertise**]

Route summarization is disabled by default.

1.8 Configuring OSPFv3 Route Filtering

1.8.1 Overview

Route filtering can prevent routes from being loaded to the routing table or advertised to neighbors. Network users cannot access the specified destination network.

Routes are filtered using the following three methods:

- When an interface is configured as a passive interface, it no longer sends or receives hello packets.
- External routes are introduced to the ASBR.
- To prevent users from accessing the specified destination network, run the **distribute-list in** command to filter routes that are computed based on the received LSAs. Only routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors.

1.8.2 Restrictions and Guidelines

- The **passive-interface** command takes effect only on OSPFv3 interfaces, not on virtual links.
- The **distribute-list out** command is used with the **redistribute** command generally. The ACL filtering rules and prefix list filtering rules are mutually exclusive in the configuration. If the ACL is used for filtering routes coming from a source, the prefix list cannot be configured to filter the same routes.
- Filtering routes by using the **distribute-list in** command affects forwarding of local routes only, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black hole routes are generated. In this case, you can run the **area filter-list** or **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

1.8.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.8.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) (Optional) Configure a passive interface.

passive-interface { **default** | *interface-type interface-number* }

The passive mode of interfaces is disabled by default, and all interfaces are allowed to send and receive OSPFv3 packets.

(5) (Optional) Configure redistributed route filtering.

distribute-list { *acl-name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

By default, the filtering function of redistributed routes is disabled, that is, all the redistributed routes pass the filtering rules.

(6) Configure learned route filtering.

distribute-list { *acl-name* | **prefix-list** *prefix-list-name* } **in** [*interface-type interface-number*]

By default, the function of filtering routes computed based on the received LSAs is disabled, that is, all these routes get passed.

1.9 Adjusting OSPFv3 Routing

1.9.1 Overview

In actual network scenario, the network administrator expects to control OSPFv3 routes so that traffic passes or bypasses some nodes or to adjust priority of a type of OSPFv3 routes.

1.9.2 Restrictions and Guidelines

There are two methods of adjusting OSPFv3 routes:

- Adjust cost values.
  - Configure the reference bandwidth.

    The default value of OSPFv3 reference bandwidth is 100 Mbps, and the cost is the actual bandwidth divided by the reference bandwidth. In the Gigabit and 10 Gigabit network environments, the computed cost value is 1, so the default bandwidth value cannot adapt to the current high-speed transport network. A router is connected to lines with different bandwidths. You are advised to adjust the configuration according to the actual bandwidth if you want to preferentially select the line with a larger bandwidth.
  - Configure the interface cost.

    Modifying the interface cost of OSPFv3 can optimize routing. A lower cost value of a link indicates a higher priority during routing.
  - Configure cost of the default route in a stub area or an NSSA.

    After an area is configured as a stub area/NSSA, the ABR will advertise the default route to the stub area/NSSA, ensuring that the routes from the stub area/NSSA to other areas are reachable. The default cost value of the default route is 1. To lower the routing priority of the default route, you can set the cost to a greater value.
  - Configure redistributed route cost.

    When redistributing external routes, you can configure the cost values of external routes to adjust routing flexibly.
- Modify the administrative distance.

  The administrative distance is used to select the best path when multiple routing protocols are used to reach the same target. Administrative distance defines the reliability of a routing protocol. A smaller administrative distance indicates higher reliability and higher routing priority. The default administrative distance values of OSPFv3 intra-domain routes, inter-domain routes, and external routes are all **110**. The administrative distance can be set to different values to control routing.

1.9.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.9.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) (Optional) Configure the reference bandwidth.

auto-cost reference-bandwidth *reference-bandwidth*

The default reference bandwidth value computed based on the metric of an interface is **100** Mbps.

(5) (Optional) Configure the interface cost.

ipv6 ospf cost *cost* [**instance** *instance-id*]

The default cost value of an OSPFv3 interface is **100** Mbps/Bandwidth. Bandwidth indicates the bandwidth of the interface and it is configured by running the **bandwidth** command in interface configuration mode. The configured bandwidth overwrites the cost automatically computed.

The default costs of OSPFv3 interfaces on several typical lines are as follows:

- For the 64 kbps serial line, the cost is **1562**.
- For the E1 line, the cost is **48**.
- For the 10 Mbps Ethernet, the cost is **10**.
- For the 100 Mbps Ethernet, the cost is **1**.

(6) (Optional) Configure the cost value of the default route in a stub area or an NSSA.

area *area-id* **default-cost** *cost*

This command takes effect only on an ABR in a stub area or on an ABR/ASBR in an NSSA.

This command must be used with the **redistribute** command. This command does not take effect on external routes that are injected to the OSPFv3 routing domain by the **default-information originate** command.

(7) (Optional) Configure the default metric for redistribution.

default-metric *metric*

The default metric of a redistributed route is **20**.

(8) (Optional) Configure an administrative distance.

distance { *distance* | **ospf** { **external** *distance* | **inter-area** *distance* | **intra-area** *distance* } * }

The default administrative distance of all OSPFv3 routes is **110**. A smaller administrative distance indicates a higher route priority. If the administrative distance of a route entry is set to **255**, the route entry is not trustworthy and does not participate in packet forwarding.

1.10 Adjusting OSPFv3 Network Convergence Speed

1.10.1 Overview

The OSPFv3 network convergence speed is controlled by adjusting the transmission time and route computation time of OSPFv3 packets.

1.10.2 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.10.3 Configuration Tasks

The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring Transmission Time of OSPFv3 Packets
- Configuring OSPFv3 Route Computation Time

1.10.4 Configuring Transmission Time of OSPFv3 Packets

1. Overview

The OSPFv3 network convergence speed is controlled by adjusting the hello packet sending interval, dead interval and LSU transmission time of an OSPFv3 interface.

2. Restrictions and Guidelines

- Hello packet sending interval
  - A shorter hello interval indicates that OSPFv3 can detect topology changes more quickly, but the network traffic increases.
  - By default, the neighbor dead interval is four times the hello packet sending interval. If the hello packet sending interval is modified, the dead interval is modified automatically.
  - The neighbor dead interval cannot be shorter than the hello packet sending interval.
  - The hello packet sending intervals and the neighbor dead intervals must be the same on all routers in the same network segment.
- Dead interval
  - The dead interval cannot be smaller than the hello packet sending interval.
  - The dead interval must be the same on all routers in the same network segment.
- The sending delay and line transmission delay of the interface must be considered when the **transmit-delay** command is configured. For a low-speed line, the transmission delay of the interface must be set to a value greater than the default value.
- If no acknowledgment is received from the neighbor within the time defined by the **retransmit-interval** command, the LSU packet is retransmitted. The retransmission delay can be set to a value greater than the default value on a serial line or virtual link to prevent unwanted retransmission.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) (Optional) Configure the hello interval.

ipv6 ospf hello-interval *hello-interval* [**instance** *instance-id*]

The default hello packet sending interval of the broadcast and P2P networks is **10** seconds. The default hello packet sending interval of the P2MP and NBMA networks is **30** seconds.

(5) (Optional) Configure the dead interval.

ipv6 ospf dead-interval { *dead-interval* | **minimal hello-multiplier** *multiplier* } [**instance** *instance-id*]

The fast hello function is disabled by default, and the neighbor dead interval is four times the sending interval of hello packets.

(6) (Optional) Configure the LSU transmission time.

ipv6 ospf transmit-delay *transmit-delay* [**instance** *instance-id*]

The default LSU packet transmission time is **1** second.

(7) (Optional) Configure the LSU retransmission interval.

ipv6 ospf retransmit-interval *retransmit-interval* [**instance** *instance-id*]

The default LSU retransmission interval is **5** seconds.

1.10.5 Configuring OSPFv3 Route Computation Time

1. Overview

OSPFv3 route convergence speed is controlled by adjusting the LSA generation time, LSA group refresh time, SPF computation time, and route computation time.

2. Restrictions and Guidelines

- LSA generation time
  - If a high requirement is raised for network convergence during link change, you can set *delay-time* to a smaller value. You can also appropriately increase the values of the preceding parameters to reduce the CPU usage.
  - The value of *hold-time* cannot be smaller than the value of *delay-time*, and the value of *max-wait-time* cannot be smaller than the value of *hold-time*.
- LSA group refresh time
  - Every LSA has a time to live (TTL) age. When the LSA age reaches 1800s, a refreshment is needed to prevent LSAs from being cleared because their ages reaching the maximum. If LSA update and aging computation are performed for every LSA, the device will consume a lot of CPU resources. To use CPU resources effectively, you can refresh LSAs by group on the device. The interval of group refreshment is called group pacing interval. The group refreshment operation is to organize the LSAs generated within a group pacing interval into a group and refresh the group as a whole.

- If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout. To maintain the CPU stability, the number of LSAs to be processed upon each timeout cannot be too large. If the number of LSAs is large, you are advised to reduce the group pacing interval. For example, if there are 10,000 LSAs in the database, you can reduce the pacing interval; if there are 40 to 100 LSAs, you can set the pacing interval to 10-20 minutes.

- LSA group sending interval

  If the number of LSAs is large and the device load is heavy in an environment, properly configuring *transimit-time* and *transimit-count* can limit the number of LS-UPD packets flooded in the network. If the CPU usage is not high and the network bandwidth load is not heavy, reducing the value of *transimit-time* and increasing the value of *transimit-count* can accelerate the environment convergence.

- SPF computation time
  - The *spf-delay* and *spf-holdtime* can be set to smaller values to accelerate topology convergence, and *spf-max-waittime* can be set to a larger value to reduce SPF computation.
  - The value of *spf-holdtime* cannot be smaller than that of *spf-delay*; otherwise, the value of *spf-holdtime* will be automatically set to the value of spf-delay.
  - The value of *spf-max-waittime* cannot be smaller than that of *spf-holdtime*; otherwise, *spf-max-waittime* will be automatically set to the value of *spf-holdtime*.
  - The configurations of **timers throttle spf** and **timers spf** are mutually overwritten.
  - When neither **timers spf** nor **timers throttle spf** is configured, the default value of **timers throttle spf** prevails.

- Computation delays of inter-area routes and external routes

  If a lot of inter-area or external routes exist in the network and the network is not stable, adjust the corresponding delays and optimize route computation to reduce the load on the device.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) (Optional) Configure the LSA generation time.

timers throttle lsa all *delay-time hold-time max-wait-time*

The default minimum delay of LSA generation is **0** ms, the minimum interval between the first update and the second update of LSA is **5000** ms, and the maximum interval between consecutive LSA updates is **5000** ms.

(5) (Optional) Configure the LSA group refresh time.

timers pacing lsa-group *update-time*

The default group refresh time of LSAs is **30** seconds.

(6) (Optional) Configure LSA group sending interval.

timers pacing lsa-transmit *transmit-time transmit-count*

The default LSA group sending interval is **40** ms, and the number of LS-UPD packets in each group is **1**.

(7) (Optional) Configure the SPF computation delay.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

The default delay for SPF computation is **1000** ms, the minimum interval between two SPF computations is **5000** ms, and the maximum interval between two SPF computations is **10000** ms.

(8) Configure the computation delays of inter-area routes and external routes.

timers throttle route { **ase** *ase-delay* | **inter-area** *ia-delay* }

The default delay for inter-area route and external route computation is **0** ms.

(9) (Optional) Configure duplicate LSA receiving delay.

timers lsa arrival *arrival-time*

The default delay for receiving a duplicate LSA is **1000** ms.

1.11 Enabling OSPFv3 Authentication

1.11.1 Overview

OSPFv3 uses the authentication mechanism, that is, IP authentication header (AH) and IP encapsulating security payload (ESP), provided by IPv6 to prevent unauthorized routers from accessing the network and hosts that forge OSPFv3 packets from participating in OSPFv3 routing.

1.11.2 Restrictions and Guidelines

- If SA authentication is configured for an area, the configuration takes effect on all interfaces that belong to this area.
- Authentication priority of OSPFv3 instances, areas, and interfaces are as follows: OSPFv3 instance authentication < area authentication < interface authentication.

1.11.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.11.4 Configuration Tasks

The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring Area Authentication and Encryption
- Configuring Interface Authentication and Encryption

1.11.5 Configuring Area Authentication and Encryption

1. Overview

When area authentication and encryption are enabled, the authentication mode and password of all devices in an area must be consistent to ensure normal setup of neighbor relationship.

2. Restrictions and Guidelines

- The device supports three authentication types:
  - No authentication (when authentication is not configured)
  - MD5
  - SHA1
- The device supports three encryption types:
  - DES
  - 3DES
  - AES-CBC
- After an OSPFv3 area is configured with encryption and authentication, the configuration takes effect on all interfaces (except virtual links) in the area, but the interface encryption and authentication configuration takes precedence over the area configuration.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) (Optional) Configure area authentication.

area *area-id* **authentication ipsec spi** *spi* { **md5** [**string-key**] | **sha1** } [**0** | **7**] *key*

The OSPFv3 area authentication function is disabled by default.

(5) (Optional) Configure area encryption.

area *area-id* **encryption ipsec spi** *spi* **esp** { { **3des** | **aes-cbc** { **128** | **192** | **256** } | **des** } [**0** | **7**] *des-key* | **null** } { **md5** | **sha1** } [**0** | **7**] *key*

Encryption is disabled by default.

1.11.6 Configuring Interface Authentication and Encryption

1. Overview

Applied between neighbor devices, interface authentication has higher priority than area authentication. The authentication mode and password for neighbor devices must be the same.

2. Restrictions and Guidelines

- The device supports three authentication types:
  - No authentication (when authentication is not configured)
  - MD5
  - SHA1

- The device supports three encryption types:
  - DES
  - 3DES
  - AES-CBC
- The OSPFv3 encryption and authentication parameters configured on interfaces must be consistent.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) (Optional) Configure interface encryption.

ipv6 ospf encryption { **ipsec spi** *spi* **esp** { { **3des** | **aes-cbc** { **128** | **192** | **256** } | **des** } [**0** | **7**] *des-key* | **null** } { **md5** | **sha1** } [**0** | **7**] *key* | **null** } [**instance** *instance-id*]

Encryption is disabled by default.

1.12 Enabling Two-Way Maintenance

1.12.1 Overview

If the two-way maintenance function is enabled, in addition to the hello packets, the DD, LSU, LSR, and LSAck packets from a neighbor can also be used to maintain the bidirectional communication between neighbors. This prevents termination of the adjacency caused by delayed or discarded hello packets.

1.12.2 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.12.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Enable two-way maintenance.

two-way-maintain

The two-way maintenance function of OSPFv3 is enabled by default.

1.13 Correlating OSPFv3 with BFD

1.13.1 Overview

The OSPFv3 protocol dynamically discovers a neighbor by using hello packets. After BFD is enabled, OSPFv3 establishes a BFD session with a neighbor in the full neighbor relationship. The neighbor state is detected using the BFD mechanism. When the BFD neighbor fails, OSFPv3 immediately performs network convergence. This configuration helps shorten the traffic interruption time.

1.13.2 Restrictions and Guidelines

- The BFD parameters must be configured for the interface in advance.
- If BFD is configured for both a process and an interface, the interface-based configuration takes effect preferentially.

1.13.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.13.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an OSPFv3 interface correlation with BFD.

a Enter the interface configuration mode.

interface *interface-type interface-number*

b Configure an OSPFv3 interface correlation with BFD.

ipv6 ospf bfd [**disable**]

The BFD function is disabled on an interface by default, and the BFD configuration is subject to the configuration in the OSFPv3 process configuration mode.

(4) Exit the interface configuration mode.

exit

(5) Configure OSPFv3 correlation with BFD.

a Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

b Configure an OSPFv3 interface correlation with BFD.

bfd all-interfaces

The BFD function is disabled on all interfaces by default.

1.14 Enabling the GR Function

1.14.1 Overview

When a GR-enabled router is restarted on the control plane, data forwarding can be still guided on the forwarding plane. In addition, actions such as neighbor relationship re-forming and route computation performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

When a router implements GR, GR helper sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper upon receiving the Grace-LSA, and helps the neighbor routers to complete GR.

1.14.2 Restrictions and Guidelines

- The neighbor router must support the GR helper.
- The GR time cannot be shorter than the neighbor relationship maintenance time of the neighbor router.

1.14.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.14.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Enable the GR function.

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

The GR function is enabled by default.

(5) Enable the OSPFv3 GR helper function.

graceful-restart helper { **disable** | **internal-lsa-checking** | **strict-lsa-checking** }

The GR helper capability is enabled by default. After the GR helper is enabled on the device, LSA changes are not checked.

1.15 Enabling NSR

1.15.1 Overview

During nonstop routing (NSR), OSPFv3-related information is backed up from the active supervisor module of a distributed device to the standby supervisor module, or from the active host of a virtual switching unit (VSU) to the standby host. In this way, the device can automatically recover the link state and re-generate routes without the help of the neighbor devices during the active/standby switchover. Information that should be backed up includes the neighbor relationship and link state.

1.15.2 Restrictions and Guidelines

- This command is used to enable the NSR function. For the same OSPFv3 process, either NSR or GR is enabled because they are mutually exclusive. Nevertheless, when NSR is enabled, the GR helper capability is supported.
- The switchover of devices in distributed or VSU mode takes a period of time. If OSPFv3 neighbor keepalive duration is shorter than the switchover duration, the OSPFv3 neighbor relationship with the neighbor device is removed, and services are interrupted during the switchover. Therefore, it is recommended that the OSPFv3 neighbor keepalive duration be no smaller than the default value when the NSR function is enabled. When the fast hello function is enabled, the OSPFv3 neighbor keepalive duration is less than 1s. As a result, it is recommended that the NSR function be disabled.

1.15.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.15.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Enable the NSR function.

nsr

The NSR function is disabled by default.

1.16 Modifying the Maximum Number of Concurrent Neighbors

1.16.1 Overview

When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum number of neighbors with which each OSPFv3 instance can concurrently initiate or accept interaction. The maximum number of neighbors can be configured at the process or device level.

1.16.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the maximum number of concurrent neighbors of all processes.

ipv6 router ospf max-concurrent-dd *number*

The maximum number of neighbors is **10** by default.

(4) Enter the OSPFv3 routing process configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(5) (Optional) Configure the maximum number of concurrent neighbors of the current process.

max-concurrent-dd *number*

The default maximum number of concurrent neighbors for a single process is **5**.

1.17 Configuring Network Management Functions

1.17.1 Overview

Use the network management software to manage OSPFv3 parameters and monitor the OSPFv3 running status.

1.17.2 Restrictions and Guidelines

- To enable the MIB function of the OSPFv3, you must enable the MIB function of the SNMP server.
- To enable the Trap function of the OSPFv3, you must enable the Trap function of the SNMP server.
- To output the OSPFv3 logs, you must enable the logging function of the device.

1.17.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.17.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Bind the MIB with an OSPFv3 process.

enable mib-binding

The MIB is bound to the OSPFv3 process with the minimum process ID by default.

(5) Configure the Trap function.

enable traps [**error** [**IfConfigError** | **IfRxBadPacket** | **VirtIfConfigError** | **VirtIfRxBadPacket**] * | **state-change** [**IfStateChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **VirtIfStateChange** | **VirtNbrStateChange** | **RestartStatusChange** | **NbrRestartHelperStatusChange** | **VirtNbrRestartHelperStatusChange**] *]

The Trap function is disabled by default.

(6) (Optional) Configure the logging function.

log-adj-changes [**detail**]

The logging function is enabled by default, without the **detail** parameter. The log records the log information of the following four types of events only: the adjacency reaches the full state; the adjacency leaves the full state; the adjacency reaches the down state; the adjacency leaves the down state.

1.18 Disabling MTU Verification

1.18.1 Overview

When receiving a DD packet, OSPFv3 verifies whether the MTU of the neighbor's interface is the same as that of its own interface. If the neighbor interface MTU specified in the local received DD packet is greater than the MTU of the local interface, the neighbor relationship cannot be set up. After this function is enabled, adjacency can be set up and the unicast routing service can be provided even if the MTUs of interfaces on neighbor routers are different.

1.18.2 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.18.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Disable MTU verification.

ipv6 ospf mtu-ignore

The MTU verification function is disabled by default.

1.19 Enabling OSPFv3 on a Super VLAN

1.19.1 Overview

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when OSPFv3 multicast packets are sent over a super VLAN containing multiple sub VLANs, the OSPFv3 multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing protocol flapping. In most scenarios, the OSPFv3 function does not need to be enabled in a super VLAN, and it is disabled by default. In some other scenarios, OSPFv3 needs to be run in the super VLAN, but packets need to be sent to only one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious when configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

1.19.2 Restrictions and Guidelines

- The specified sub VLAN must be connected to neighbors.

1.19.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.19.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *vlan vlan-id*

(4) Configure OSPFv3 to run on a super VLAN.

ipv6 ospf subvlan [**all** | *vlan-id*]

The OSPFv3 function takes effect in super VLANs only and is disabled by default.

1.20 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

Running the **clear** command may lose vital information and thus interrupt services.

Table 1-8 Monitoring

Command	Purpose
show ipv6 ospf [*process-id*]	Displays the configuration information of the OSPFv3 process.
show ipv6 ospf [*process-id*] **database** [*lsa-type* [**adv-router** *router-id*]]	Displays the OSPFv3 LSDB.
show ipv6 ospf [*process-id*] **interface** [*interface-type interface-number* | **brief**]	Displays the OSPFv3 interface.
show ipv6 ospf [*process-id*] **neighbor** [*interface-type interface-number* [**detail**] | *neighbor-id* | **detail**]	Displays the neighbor list of OSPFv3.

Command	Purpose
show ipv6 ospf [*process-id*] **route** [**count**]	Displays the OSPFv3 routing table.
show ipv6 ospf [*process-id*] **summary-prefix**	Displays the summarized routes of OSPFv3 redistributed routes.
show ipv6 ospf [*process-id*] **topology** [**area** *area-id*]	Displays the OSPFv3 network topology information.
show ipv6 ospf [*process-id*] **virtual-links**	Displays the OSPFv3 virtual links.
clear ipv6 ospf [*process-id*] **process**	Clears and resets the OSPFv3 process.
debug ipv6 ospf events [**abr** | **asbr** | **os | nssa** | **router** | **vlink**]	Debugs the OSPFv3 events.
debug ipv6 ospf ifsm [**events** | **status** | **timers**]	Debugs the OSPFv3 interfaces.
debug ipv6 ospf nfsm [**events** | **status** | **timers**]	Debugs the OSPFv3 neighbors.
debug ipv6 ospf nsm [**interface** | **redistribute** | **route**]	Debugs the OSPFv3 NSM.
debug ipv6 ospf lsa [**flooding** | **generate** | **install** | **maxage** | **refresh**]	Debugs the OSPFv3 LSAs.
debug ipv6 ospf packet [**dd | detail** | **hello** | **ls-ack** | **ls-request** | **ls-update** | **recv** | **send**]	Debugs the OSPFv3 packets.
debug ipv6 ospf route [**ase** | **ia** | **install** | **spf** | **time**]	Debugs the OSPFv3 routes.

1.21 Configuration Examples

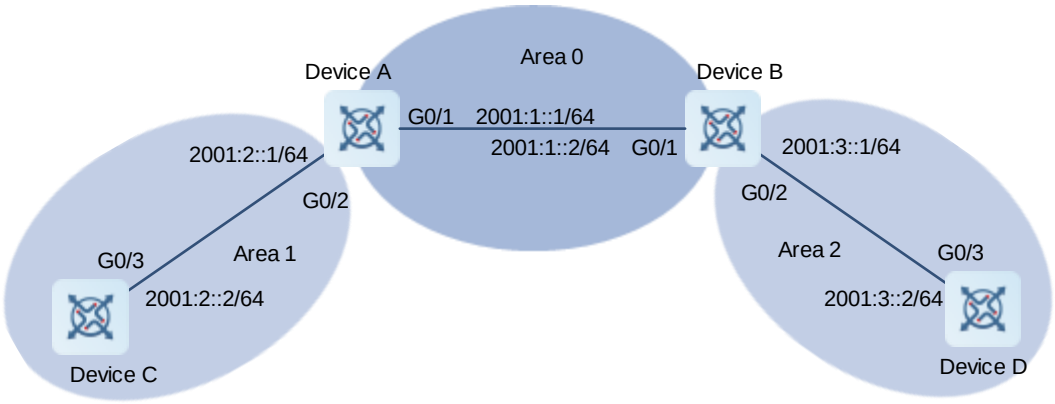
1.21.1 Configuring Basic Functions of OSPFv3

1. Requirements

OSPFv3 is enabled on all the devices, and three areas are defined in total. Device A and device B are used as ABRs forwarding inter-area routes so as to implement the interworking between all networks.

2. Topology

Figure 1-9 Topology of Basic SNMPv3 Function



3. Notes

- Configure interface IP addresses on all the devices.
- Enable the IPv4 unicast routing function on all the devices. (This function is enabled by default.)
- Configure OSPFv3 instances and router IDs on all the devices.
- Configure OSPFv3 on interfaces of all the devices.

4. Procedure

(1) Perform the following configurations on Device A.

Enable the OSPFv3 process and configure a router ID.

```
Device A> enable
Device A# configure terminal
Device A(config)# ipv6 router ospf 1
Device A(config-router)# router-id 1.1.1.1
Device A(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 enable
Device A(config-if-GigabitEthernet 0/1)# ipv6 address 2001:1::1/64
Device A(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface gigabitethernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ipv6 enable
Device A(config-if-GigabitEthernet 0/2)# ipv6 address 2001:2::1/64
Device A(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 1
Device A(config-if-GigabitEthernet 0/2)# exit
```

(2) Perform the following configurations on Device B.

Enable the OSPFv3 process and configure a router ID.

```
Device B> enable
Device B# configure terminal
Device B(config)# ipv6 router ospf 1
Device B(config-router)# router-id 2.2.2.2
Device B(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ipv6 enable
Device B(config-if-GigabitEthernet 0/1)# ipv6 address 2001:1::2/64
Device B(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface gigabitethernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ipv6 enable
Device B(config-if-GigabitEthernet 0/2)# ipv6 address 2001:3::1/64
Device B(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 2
Device B(config-if-GigabitEthernet 0/2)# exit
```

(3) Perform the following configurations on Device C.

Enable the OSPFv3 process and configure a router ID.

```
Device C> enable
Device C# configure terminal
Device C(config)# ipv6 router ospf 1
Device C(config-router)# router-id 3.3.3.3
Device C(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
Device C(config)# interface gigabitethernet 0/3
Device C(config-if-GigabitEthernet 0/3)# ipv6 enable
Device C(config-if-GigabitEthernet 0/3)# ipv6 address 2001:2::2/64
Device C(config-if-GigabitEthernet 0/3)# ipv6 ospf 1 area 1
Device C(config-if-GigabitEthernet 0/3)# exit
```

(4) Perform the following configurations on Device D.

Enable the OSPFv3 process and configure a router ID.

```
Device D> enable
Device D# configure terminal
Device D(config)# ipv6 router ospf 1
Device D(config-router)# router-id 4.4.4.4
Device D(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
Device D(config)# interface gigabitethernet 0/3
Device D(config-if-GigabitEthernet 0/3)# ipv6 enable
Device D(config-if-GigabitEthernet 0/3)# ipv6 address 2001:3::2/64
Device D(config-if-GigabitEthernet 0/3)# ipv6 ospf 1 area 2
Device D(config-if-GigabitEthernet 0/3)# exit
```

5. Verification

(1) Display the following information on Device A.

Display OSPFv3 neighbor information.

```
Device A# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State          Dead Time   Instance ID   Interface
2.2.2.2          1   Full/BDR        00:00:30    0            GigabitEthernet 0/1
3.3.3.3          1   Full/BDR        00:00:35    0            GigabitEthernet 0/2
```

Display OSPFv3 routing table.

```
Device A# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O  IA  2001:3::/64 [110/20] via FE80::2D0:F8FF:FE22:4524, GigabitEthernet 0/1
```

(2) Display the following information on Device B.

Display OSPFv3 neighbor information.

```
Device B# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State          Dead Time   Instance ID   Interface
1.1.1.1          1   Full/DR         00:00:30    0            GigabitEthernet 0/1
4.4.4.4          1   Full/BDR        00:00:35    0            GigabitEthernet 0/2
```

Display OSPFv3 routing table.

```
Device B# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O  IA  2001:2::/64 [110/20] via FE80::2D0:F8FF:FE22:4536, GigabitEthernet 0/1
```

(3) Display the following information on Device C.

Display OSPFv3 neighbor information.

```
Device C# show ipv6 ospf neighbor
```

```
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
1.1.1.1          1   Full/DR         00:00:30    0            GigabitEthernet 0/3
```

Display OSPFv3 routing table.

```
Device C# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O  IA  2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3
O  IA  2001:3::/64 [110/3] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3
```

(4) Display the following information on Device D.

Display OSPFv3 neighbor information.

```
Device D# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
2.2.2.2          1   Full/DR         00:00:30    0            GigabitEthernet 0/3
```

Display OSPFv3 routing table.

```
Device D# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O  IA  2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3
O  IA  2001:2::/64 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3
```

Verify that 2001:2::2/64 can be pinged successfully on Device D.

```
Device D# ping 2001:2::2
Sending 5, 100-byte ICMP Echoes to 2001:2::2, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/9/14 ms.
```

6. Configuration Files

- Device A configuration file

```
!
ipv6 router ospf 1
 router-id 1.1.1.1
!
interface gigabitethernet 0/1
 ipv6 enable
 ipv6 address 2001:1::1/64
 ipv6 ospf 1 area 0
!
interface gigabitethernet 0/2
 ipv6 enable
 ipv6 address 2001:2::1/64
 ipv6 ospf 1 area 1
!
```

- Device B configuration file

```
!
ipv6 router ospf 1
 router-id 2.2.2.2
!
interface gigabitethernet 0/1
 ipv6 enable
 ipv6 address 2001:1::2/64
 ipv6 ospf 1 area 0
!
interface gigabitethernet 0/2
 ipv6 enable
 ipv6 address 2001:3::1/64
 ipv6 ospf 1 area 2
!
```

- Device C configuration file

```
!
ipv6 router ospf 1
 router-id 3.3.3.3
!
interface gigabitethernet 0/3
 ipv6 enable
 ipv6 address 2001:2::2/64
 ipv6 ospf 1 area 1
!
```

- Device D configuration file

```
!
ipv6 router ospf 1
 router-id 4.4.4.4
!
interface gigabitethernet 0/3
```

```
 ipv6 enable
 ipv6 address 2001:3::2/64
 ipv6 ospf 1 area 2
!
```

7. Common Errors

- No IPv6 address is configured for the interface.
- OSPFv3 cannot be enabled because the IPv6 unicast routing function is disabled.
- The area IDs configured for adjacent interfaces are inconsistent.
- The same router ID is configured on multiple devices, resulting in a router ID conflict.

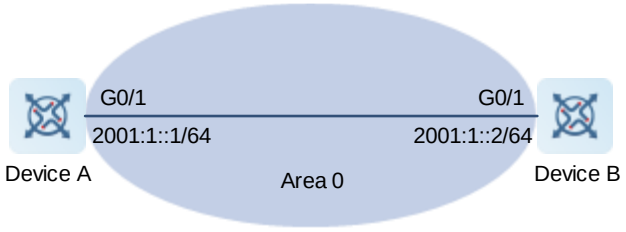
1.21.2 Configuring OSPFv3 Authentication

1. Requirements

OSPFv3 runs between Device A and Device B. MD5 authentication is configured to improve security of an OSPFv3 network.

2. Topology

Figure 1-10 Topology of OSPFv3 Authentication



3. Notes

Configure MD5 authentication on interfaces of all the devices.

4. Procedure

(1) Configure basic OSPFv3 functions (omitted).

(2) Enable OSPFv3 authentication on an interface.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 ospf authentication ipsec spi 256 md5
01234567890123456789012345678912
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
```

```
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ipv6 ospf authentication ipsec spi 256 md5
01234567890123456789012345678912
```

5. Verification

Verify whether neighbors of Device A and Device B are established.

- Check the neighbor information of Device A.

```
Device A# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
2.2.2.2          1   Full/DR         00:00:38    0            GigabitEthernet 0/1
```

- Check the neighbor information of Device B.

```
Device B# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State           Dead Time   Instance ID   Interface
1.1.1.1          1   Full/BDR        00:00:38    0            GigabitEthernet 0/1
```

6. Configuration Files

- Device A configuration file

```
!
interface gigabitethernet 0/1
  ipv6 ospf authentication ipsec spi 256 md5 01234567890123456789012345678912
!
```

- Device B configuration file

```
!
interface gigabitethernet 0/1
  ipv6 ospf authentication ipsec spi 256 md5 01234567890123456789012345678912
!
```

7. Common Errors

- The configured authentication modes are inconsistent.
- The configured authentication keys are inconsistent.

1.21.3 Configuring a Stub Area

1. Requirements

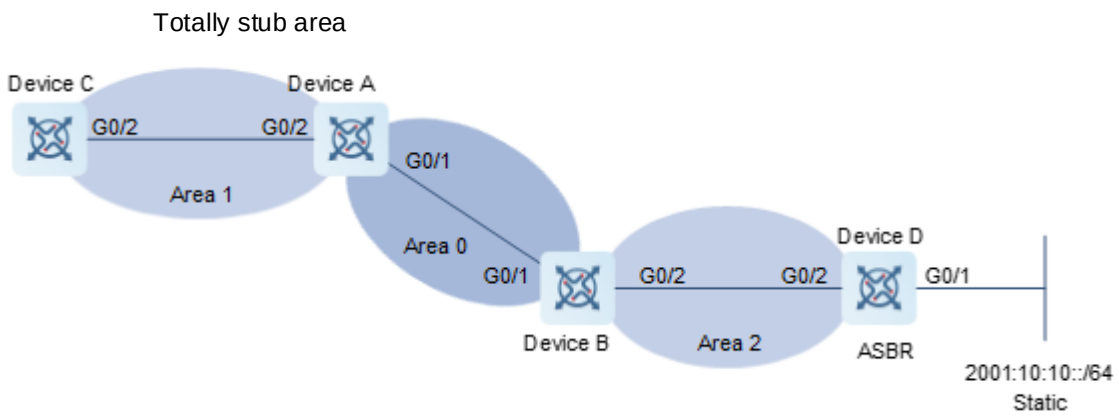
Devices A, B, C, and D are interconnected through the OSPFv3 routing protocol.

As ABRs, Devices A and B are responsible for the routing information transfer between OSPFv3 areas, and Device D functions as an ASBR to introduce the external static routes.

To reduce the number of LSAs in Area 1 and save the device performance, Area 1 is configured as a totally stub area.

2. Topology

Figure 1-11 Topology for a Stub Area



3. Notes

- Configure IPv6 addresses on interfaces of all the devices.
- Configure the basic OSPFv3 functions for all the devices.
- Introduce an external static route to Device D.
- Configure Area 1 as a stub area on Device A and Device C.

4. Procedure

(1) Configure IPv6 addresses on interfaces of all the devices and enable basic OSPFv3 functions (omitted).

(2) Introduce an external static route to Device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# ipv6 router ospf 1
Device D(config-router)# redistribute static
```

(3) Configure Area 1 as a stub area on Device A and filter Type 3 LSAs.

```
Device A> enable
Device A# configure terminal
Device A(config)# ipv6 router ospf 1
Device A(config-router)# area 1 stub no-summary
```

(4) Configure Area 1 as a stub area on Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# ipv6 router ospf 1
Device C(config-router)# area 1 stub
```

5. Verification

Run the **show ipv6 route ospf** command on Device C to display the routing table. Verify that there is only one default inter-area route, and no external static route is introduced from Device D.

```
Device C# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O  IA::/0 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2
```

6. Configuration Files

- Device A configuration file

```
!
ipv6 router ospf 1
area 1 stub no-summary
!
```

- Device C configuration file

```
!
ipv6 router ospf 1
area 1 stub
!
```

- Device D configuration file

```
!
ipv6 router ospf 1
redistribute static
!
```

7. Common Errors

- Configurations of the area type are inconsistent on devices in the same area.
- External routes cannot be introduced because route redistribution is configured on a device in the stub area.

1.21.4 Configuring an NSSA

1. Requirements

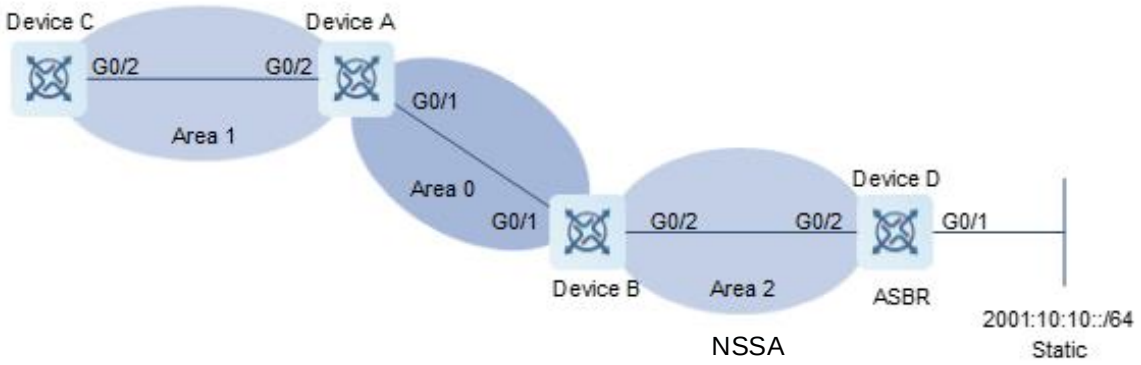
Devices A, B, C, and D are interconnected through the OSPFv3 routing protocol.

As ABRs, Devices A and B are responsible for the routing information transfer between OSPFv3 areas, and Device D functions as an ASBR to introduce the external static routes.

To reduce the number of LSAs in Area 2 and save the device performance, Area 2 is configured as an NSSA.

2. Topology

Figure 1-12 Topology for an NSSA



3. Notes

- Configure IPv6 addresses on interfaces of all the devices.
- Configure the basic OSPFv3 functions for all the devices.
- Introduce an external static route to Device D.
- Configure Area 2 as an NSSA on Device B and Device D.

4. Procedure

(1) Configure IPv6 addresses on interfaces of all the devices and enable basic OSPFv3 functions (omitted).

(2) Introduce an external static route to Device D. Configure Area 2 as an NSSA.

```
Device D> enable
Device D# configure terminal
Device D(config)# ipv6 router ospf 1
Device D(config-router)# area 2 nssa
Device D(config-router)# redistribute static
```

(3) Configure Area 2 as an NSSA on Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# ipv6 router ospf 1
Device B(config-router)# area 2 nssa
```

5. Verification

(1) Run the **show ipv6 ospf database** command on Device D to display the database information and verify that Type 7 LSAs are generated.

```
Device D# show ipv6 ospf database nssa-external
          OSPFv3 Router with ID (1.1.1.1) (Process 1)
             NSSA-external-LSA (Area 0.0.0.1)
  LS age: 1196
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.3
```

```
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000004
  Checksum: 0x1F25
  Length: 52
     Metric Type: 2 (Larger than any link state path)
     Metric: 20
Prefix: 2001:10::/64
Prefix Options: 8 (P|-|-|-)
Forwarding Address: 4000::1
```

(2) Run the **show ipv6 route ospf** command on Device A to display the routing table and verify that an external static route is introduced by Router D.

```
Device A# show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O  N2  2001:10::/64 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1
```

6. Configuration Files

- Device B configuration file

```
!
ipv6 router ospf 1
area 2 nssa
!
```

- Device D configuration file

```
!
ipv6 router ospf 1
area 2 nssa
 redistribute static
!
```

7. Common Errors

- Configurations of the area type are inconsistent on devices in the same area.

1.21.5 Selecting an OSPFv3 DR

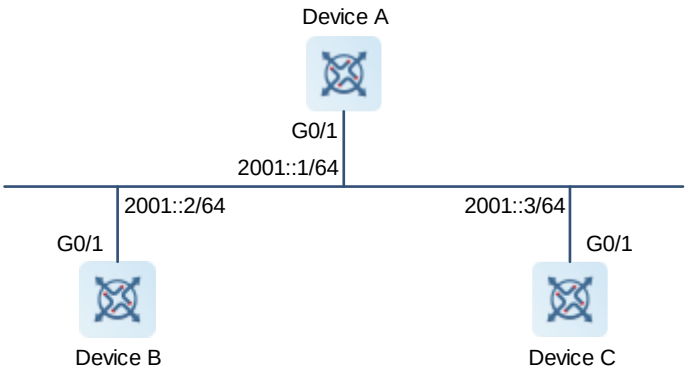
1. Requirements

Devices A, B, and C are in the same broadcast network.

The priority of Device A is set to 10 and Device A is configured as a DR. The priority of Device B is set to 5 and Device B is configured as a BDR. The priority of Device C is set to 0 and Device C does not participate in DR election.

2. Topology

Figure 1-13 Topology of OSPFv3 DR Configuration



3. Notes

- Configure IPv6 addresses on interfaces of all the devices.
- Configure the basic OSPFv3 functions for all the devices.
- Modify the DR election priority of all the devices.

4. Procedure

(1) Configure basic functions of OSPFv3.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# ipv6 router ospf 1
Device A(config-router)# router-id 1.1.1.1
Device A(config-router)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# ipv6 router ospf 1
Device B(config-router)# router-id 2.2.2.2
Device B(config-router)# exit
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# ipv6 router ospf 1
Device C(config-router)# router-id 3.3.3.3
Device C(config-router)# exit
```

(2) Configure IP addresses of interfaces, configure OSPFv3, and modify the DR election priority of all the devices.

Configure Device A.

```
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 address 2001::1/64
Device A(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device A(config-if-GigabitEthernet 0/1)# ipv6 ospf priority 10
```

Configure Device B.

```
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ipv6 address 2001::2/64
Device B(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device B(config-if-GigabitEthernet 0/1)# ipv6 ospf priority 5
```

Configure Device C.

```
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ipv6 address 2001::3/64
Device C(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device C(config-if-GigabitEthernet 0/1)# ipv6 ospf priority 0
```

5. Verification

- Run the **show ipv6 ospf interface** command on Device C to display the DR and BDR.

```
Device C# show ipv6 ospf interface
GigabitEthernet 0/1 is up, line protocol is up
  Interface ID 4098
  IPv6 Prefixes
    fe80::250:56ff:feb5:820b/64 (Link-Local Address)
    2001::3/64
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
    Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DROther, Priority 0
    Designated Router (ID) 1.1.1.1
      Interface Address fe80::250:56ff:feb5:694e
    Backup Designated Router (ID) 2.2.2.2
      Interface Address fe80::250:56ff:feb5:fdb4
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Neighbor Count is 2, Adjacent neighbor count is 2
  Hello received 73 sent 39, DD received 8 sent 7
  LS-Req received 1 sent 2, LS-Upd received 9 sent 5
  LS-Ack received 5 sent 5, Discarded 6
```

- Run the **show ipv6 ospf neighbor** command on Device A to display DROther of the broadcast network as Device C.

```
Device A# show ipv6 ospf neighbor

OSPFv3 Process (1), 2 Neighbors, 2 is Full:
```

```
Neighbor ID     Pri   State          BFD State  Dead Time    Instance ID
Interface
2.2.2.2          5   Full/BDR        -         00:00:36    0
GigabitEthernet 0/1
3.3.3.3          0   Full/DROther     -         00:00:38    0
GigabitEthernet 0/1
```

6. Configuration Files

- Device A configuration file

```
!
interface gigabitethernet 0/1
ipv6 address 2001::1/64
ipv6 ospf priority 10
ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 1.1.1.1
 graceful-restart
!
```

- Device B configuration file

```
!
interface gigabitethernet 0/1
 ipv6 address 2001::2/64
ipv6 ospf priority 5
 ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 2.2.2.2
 graceful-restart
!
```

- Device C configuration file

```
!
interface gigabitethernet 0/1
ipv6 address 2001::3/64
 ipv6 ospf priority 0
 ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 3.3.3.3
 graceful-restart
!
```

1.21.6 Configuring BFD for OSPFv3

1. Requirements

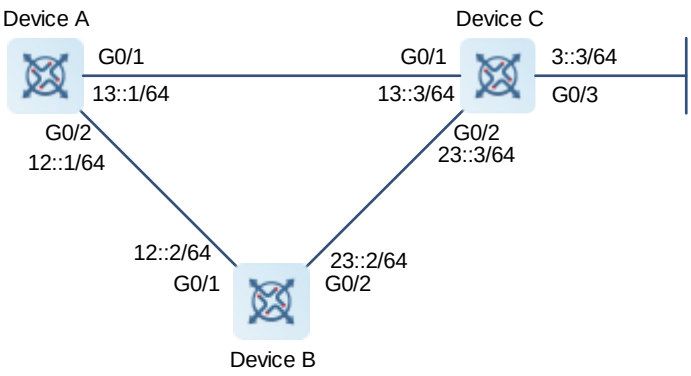
Devices A, B, and C are interconnected through OSPFv3.

The active link from Device A to 3::3 is Device A > Device C, and the standby link is Device A > Device B > Device C.

When the link from Device A to Device C fails, BFD can detect the failure and notify OSPFv3 of the failure, and quickly switch to the standby link.

2. Topology

Figure 1-14 Topology of BFD for OSPFv3



3. Notes

- Configure IPv6 addresses on interfaces of all the devices.
- Configure the basic OSPFv3 functions for all the devices.
- Enable the BFD function in the OSPFv3 routing process mode.

4. Procedure

(1) Configure IP addresses for interfaces and configure basic OSPFv3 functions.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitethernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ipv6 address 12::1/64
Device A(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 0
Device A(config-if-GigabitEthernet 0/2)# exit
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 address 13::1/64
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# ipv6 router ospf 1
Device A(config-router)# router-id 1.1.1.1
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ipv6 address 12::2/64
```

```
Device B(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface gigabitethernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ipv6 address 23::2/64
Device B(config)# ipv6 router ospf 1
Device B(config-router)# router-id 2.2.2.2
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ipv6 address 13::3/64
Device C(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface gigabitethernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ipv6 address 23::3/64
Device C(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 0
Device C(config-if-GigabitEthernet 0/2)# exit
Device C(config)# ipv6 router ospf 1
Device C(config-router)# router-id 3.3.3.3
```

(2) Enable the BFD function in the OSPFv3 routing process mode.

Configure Device A.

```
Device A(config-router)# bfd all-interfaces
```

Configure Device B.

```
Device B(config-router)# bfd all-interfaces
```

Configure Device C.

```
Device C(config-router)# bfd all-interfaces
```

5. Verification

- Normal network environment

Check the routing table of Device A.

```
Device A# show ipv6 route ospf

IPv6 routing table name - Default - 11 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, N - Nd to host

O     3::3/128 [110/1] via FE80::2D0:F8FF:FE22:358D, GigabitEthernet 0/1
O     23::/64 [110/2] via FE80::2D0:F8FF:FE22:358D, GigabitEthernet 0/1
             [110/2] via FE80::274:9CFF:FEEE:53CB, GigabitEthernet 0/2
```

Run **traceroute 3::3** on Device A.

```
Device A# traceroute 3::3
  < press Ctrl+C to break >
Tracing the route to 3::3

 1                              3::3     5 msec    8 msec   10 msec
```

- Link from Device A to Device C fails

  Check the routing table of Device A.

```
Device A# show ipv6 route ospf

IPv6 routing table name - Default - 7 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, N - Nd to host

O     3::3/128 [110/2] via FE80::274:9CFF:FEEE:53CB, GigabitEthernet 0/2
O     23::/64 [110/2] via FE80::274:9CFF:FEEE:53CB, GigabitEthernet 0/2
```

Run **traceroute 3::3** on Device A.

```
Device A# traceroute 3::3
  < press Ctrl+C to break >
Tracing the route to 3::3

 1                             12::2     6 msec    9 msec    9 msec
 2                              3::3     7 msec    9 msec   10 msec
```

6. Configuration Files

- Device A configuration file

```
!
interface gigabitethernet 0/1
ipv6 address 13::1/64
ipv6 ospf 1 area 0
!
interface gigabitethernet 0/2
ipv6 address 12::1/64
ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 1.1.1.1
 graceful-restart
 bfd all-interfaces
!
```

- Device B configuration file

```
!
interface gigabitethernet 0/1
ipv6 address 12::2/64
ipv6 ospf 1 area 0
!
interface gigabitethernet 0/2
ipv6 address 23::2/64
ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 2.2.2.2
 graceful-restart
 bfd all-interfaces
!
```

- Device C configuration file

```
!
interface gigabitethernet 0/1
ipv6 address 13::3/64
ipv6 ospf 1 area 0
!
interface gigabitethernet 0/2
ipv6 address 23::3/64
ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 3.3.3.3
 graceful-restart
 bfd all-interfaces
!
```

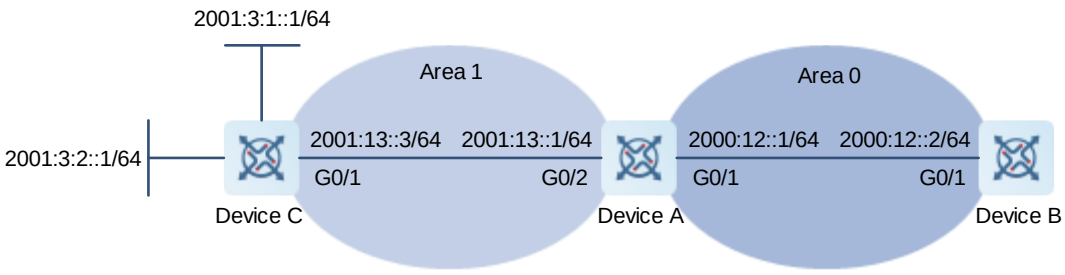
1.21.7 Configuring OSPFv3 Route Summarization

1. Requirements

Devices A and B reside in OSPFv3 Area 0, and Devices A and C reside in OSPFv3 Area 1. Two static routes are introduced to Device C. To reduce the number of routing entries, Device C summarizes introduced static routes as 2001:3::/32 and advertises the routes to the OSPFv3 domain. Device A summarizes routes in Area 1 as 2001:13::/32 and advertises the routes to the OSPFv3 neighbors.

2. Topology

Figure 1-15 Topology of OSPFv3 Route Summarization



3. Notes

- Configure IPv6 addresses on interfaces of all the devices.
- Configure the basic OSPFv3 functions for all the devices.
- Redistribute two static routes on Device C and configure external route summarization.
- Summarize routes in Area 1 on Device A.

4. Procedure

(1) Configure basic functions of OSPFv3 (omitted).

(2) Redistribute two static routes on Device C and summarize the redistributed routes as 2001:3::/32.

```
Device C> enable
Device C# configure terminal
Device C(config)# ipv6 router ospf 1
Device C(config-router)# redistribute static
Device C(config-router)# summary-prefix 2001:3::/32
```

(3) Summarize routes in Area 1 as 2001:13::/32 on Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# ipv6 router ospf 1
Device A(config-router)# area 1 range 2001:13::/32
```

5. Verification

- Display OSPFv3 routes on Device A. Summarized static routes are displayed, and route details cannot be displayed.

```
Device A# show ipv6 route ospf

IPv6 routing table name - Default - 11 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       IA - Inter area, EV - BGP EVPN, N - Nd to host

O  E2  2001:3::/32 [110/20] via FE80::250:56FF:FEB5:7BF5, GigabitEthernet 0/2
O     2001:13::/32 [110/0] via ::1, Null0
```

- Display OSPFv3 routes on Device B. Area 1 summarized routes are displayed, and route details cannot be displayed.

```
Device B# show ipv6 route ospf

IPv6 routing table name - Default - 7 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPFv3, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPFv3 NSSA external type 1, N2 - OSPFv3 NSSA external type 2
       E1 - OSPFv3 external type 1, E2 - OSPFv3 external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, N - Nd to host

O  E2  2001:3::/32 [110/20] via FE80::250:56FF:FEB5:694E, GigabitEthernet 0/1
O  IA  2001:13::/32 [110/2] via FE80::250:56FF:FEB5:694E, GigabitEthernet 0/1
```

6. Configuration Files

- Device A configuration file

```
!
 router-id 1.1.1.1
 graceful-restart
 area 1 range 2001:13::/32
!
```

- Device C configuration file

```
!
 router-id 3.3.3.3
 graceful-restart
 redistribute static
 summary-prefix 2001:3::/32
!
```

Contents

1 Configuring IS-IS 1
1.1 Overview 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 13
1.2 Restrictions and Guidelines 14
1.3 Configuration Task Summary 14
1.4 Configuring Basic Settings of IS-IS 15
1.4.1 Overview 15
1.4.2 Restrictions and Guidelines 15
1.4.3 Procedure 15
1.5 Configuring IS-IS network Levels 16
1.5.1 Overview 16
1.5.2 Restrictions and Guidelines 16
1.5.3 Procedure 16
1.6 Configuring IS-IS Hello Packets 17
1.6.1 Overview 17
1.6.2 Procedure 17
1.7 Configuring IS-IS LSPs 18
1.7.1 Overview 18
1.7.2 Restrictions and Guidelines 18
1.7.3 Procedure 18

1.8 Configuring IS-IS SNPs 20
1.8.1 Overview 20
1.8.2 Restrictions and Guidelines 20
1.8.3 Procedure 20
1.9 Configuring IS-IS Route Advertisement 21
1.9.1 Overview 21
1.9.2 Restrictions and Guidelines 21
1.9.3 Procedure 21
1.10 Configuring IS-IS Route Summarization 22
1.10.1 Overview 22
1.10.2 Procedure 22
1.11 Configuring an IS-IS Passive Interface 23
1.11.1 Overview 23
1.11.2 Restrictions and Guidelines 23
1.11.3 Procedure 23
1.12 Controlling IS-IS Routing Factors 23
1.12.1 Overview 23
1.12.2 Restrictions and Guidelines 23
1.12.3 Procedure 24
1.13 Configuring the Priority of an IS-IS Device 25
1.13.1 Overview 25
1.13.2 Restrictions and Guidelines 25
1.13.3 Procedure 25
1.14 Configuring IS-IS Authentication 25

1.14.1 Overview 25

1.14.2 Restrictions and Guidelines 25

1.14.3 Procedure 26

1.15 Configuring IS-IS GR 28

1.15.1 Overview 28

1.15.2 Restrictions and Guidelines 28

1.15.3 Procedure 28

1.16 Configuring IS-IS NSR 29

1.16.1 Overview 29

1.16.2 Restrictions and Guidelines 29

1.16.3 Procedure 29

1.17 Correlating IS-IS with BFD 30

1.17.1 Overview 30

1.17.2 Restrictions and Guidelines 30

1.17.3 Procedure 30

1.18 Configuring the IS-IS Overload Bit 31

1.18.1 Overview 31

1.18.2 Restrictions and Guidelines 31

1.18.3 Procedure 32

1.19 Configuring IS-IS VRF 32

1.19.1 Overview 32

1.19.2 Restrictions and Guidelines 32

1.19.3 Procedure 33

1.20 Configuring IS-IS MTR 33

1.20.1 Overview 33

1.20.2 Restrictions and Guidelines 33

1.20.3 Procedure 33

1.21 Configuring IS-IS SNMP 33

1.21.1 Overview 33

1.21.2 Restrictions and Guidelines 34

1.21.3 Procedure 34

1.22 Enabling Super VLAN for IS-IS 34

1.22.1 Overview 34

1.22.2 Restrictions and Guidelines 35

1.22.3 Procedure 35

1.23 Configuring IS-IS Two-way Maintenance 35

1.23.1 Overview 35

1.23.2 Restrictions and Guidelines 35

1.23.3 Procedure 35

1.24 Configuring Extended Feature of IS-IS 36

1.24.1 Overview 36

1.24.2 Configuration Tasks 36

1.24.3 Configuring the Maximum Metric of a Neighbor 36

1.24.4 Configuring the Maximum Number of Area Addresses 37

1.24.5 Configuring SPF Calculation Interval 37

1.24.6 Canceling Three-Way Handshake of a P2P Network 38

1.24.7 Enabling TLV to Be Padded Based on Supported Protocol 38

1.24.8 Configuring the Reachable Time of a Suppressed Neighbor 39

1.24.9 Enabling Adjacency Event Output 40

1.25 Monitoring 40

1.26 Configuration Examples..... 42

1.26.1 Performing Basic Authentication Configuration of IS-IS..... 42

1.26.2 Configuring IS-IS MTR..... 47

1.26.3 Configuring IS-IS Route Summarization..... 54

1.26.4 Correlating IS-IS with BFD..... 56

1 Configuring IS-IS

1.1 Overview

1.1.1 Overview

Intermediate System to Intermediate System (IS-IS) is an extensible, robust, and easy-to-use Interior Gateway Protocol (IGP) for route selection and applicable to an IP and ISO (connectionless network service) CLNS dual environment network.

IS-IS was designed for the Connection-Less Network Protocol (CLNP) at the very start. After TCP/IP became mainstream protocols, IETF modified IS-IS so that this protocol could apply to TCP/IP environment. The modified IS-IS is referred to as Integrated IS-IS or Dual IS-IS.

IS-IS has the common characteristics of a link state protocol. It sends Hello packets to discover and maintain neighbor relationships, and sends Link State Protocol Data Units (LSPs) to neighbors to advertise its link state. IS-IS supports Level-1 routing and Level-2 routing. All devices at the same level maintain the same link state database (LSDB), which stores the LSPs generated by the devices to notify each other of the network topology at this level. Each device uses the Dijkstra shortest path first (SPF) algorithm to perform best-route computation, path selection, and fast convergence.

Note

In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be Layer-3 switches, routers, or firewalls.

1.1.2 Principles

1. Basic Concepts

- IS-IS network hierarchy

  As shown in Figure 1-1, an IS-IS network is divided into Level-1 and Level-2. The nodes on which devices exchange information in the same area form one level (Level-1).

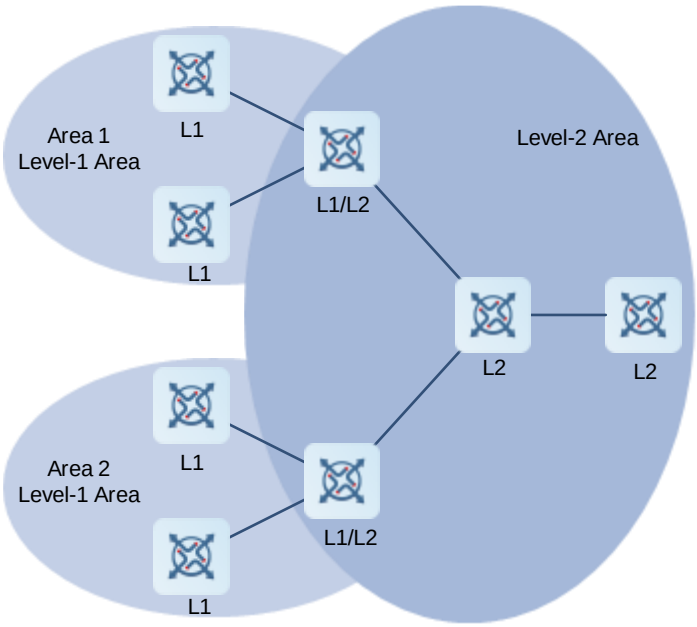
  - Level-1 routers perform routing in the local area and they can form neighbor relationship with local Level-1 routers and Level-1/Level-2 routers and maintain Level-1 LSDB. This LSDB includes routing information of local area and packets destined for another area are forwarded to the closest Level-1/Level-2 router.
  - Level-2 routers perform inter-area routing and they can form neighbor relationship with Level-2 routers in the same area or another area and Level-1/Level-2 routers and maintain Level-2 LSDB. This LSDB includes inter-area routing information. All Level-2 routers and Level-1/Level-2 routers form a backbone network of a routing domain and take charge of communication between different areas. The backbone network must be physically connected. Only Level-2 routers can exchange data packets and routing information with routers outside the routing domain.
  - Level-1/Level-2 routers, belonging to Level-1 and Level-2 areas, can form Level-1 neighbor relationship with Level-1 routers in the same area and Level-1/Level-2 routers and form Level-2 neighbor

relationship with Level-2 routers in the same or another area and Level-1/Level-2 routers. Level-1 routers must be connected to another area through Level-1/Level-2 routers. Level-1/Level-2 routers maintain two LSDBs. Level-1 LSDB is used for internal routing, and Level-2 LSDB is used for inter-area routing. By default, Level-1/Level-2 routers redistribute Level-1 routes to Level-2 routers. If there are many Level-1 routes, the routes must be summarized and then redistributed to Level-2 routers.

All devices in an area know the network topology of the area and exchange data within the area. Level-1/Level-2 devices are border devices that belong to different areas and provide inter-area connections. Areas are connected by Level-2 devices. The border devices in various areas form a Level-2 backbone network for inter-area data exchange.

Level-1 devices are only interested in the local area's topology, including all nodes in the local area and the next-hop devices destined for the nodes. Level-1 devices access other areas through Level-2 devices and forward packets from a target network outside the local area to the closest Level-2 device.

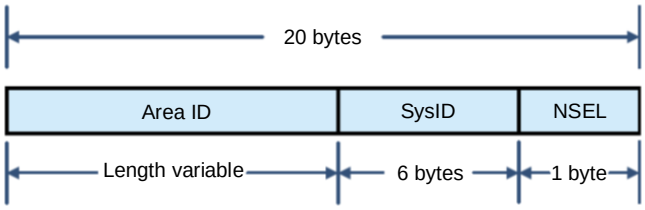
Figure 1-1 IS-IS Network Architecture



- IS-IS address coding mode

  An IS-IS address is called a network entity title (NET) and it consists of an area ID, a system ID, and a network service access point (NSAP) ID. An IS-IS address ranges from 8 to 20 bytes.

Figure 1-2 NET Address Format



  - The area ID identifies the routing domain length in an area and is fixed relative to the routing domain. It

ranges from 1 to 13 bytes.

The area ID consists of an authority and format identifier (AFI), an initial domain identifier (IDI), and a high order DSP (HODSP). The AFI represents an address assignment authority and address format, the IDI is used to identify a domain, and the HODSP is used to distinguish areas.

- The system ID is unique in an autonomous system (AS).

  Generally, a router ID (for example, 192.168.10.1) is translated to a system ID by extending each decimal in an IP address to three decimals. For if the decimals are less than three, 0 is added for supplementation. An extended IP address is 192.168.010.001. After the extended IP address is divided into three parts, the system ID is 1921.6801.0001.

- The NSAP is a network selector and sometimes called SEL. In IS-IS, SEL is typically set to 00 to indicate a device.

- IS-IS packet types

  There are three types of IS-IS packets:

  - LSPs

    LSPs are used to transmit link state records within an area and are classified into Level-1 LSPs and Level-2 LSPs. LSPs are only flooded at the local level.

  - IS-to-IS Hello (IIH) PDUs

    IIH PDUs are used to maintain adjacency. They carry multicast MAC addresses used to determine whether other systems run IS-IS.

  - Sequence number PDUs (SNPs), including complete SNP (CSNP) and partial SNP (PSNP)

    CSNPs are used for LSDB synchronization. By default, a designated IS (DIS) sends a CSNP every 10s in a broadcast network. In a P2P network, a CSNP is sent only after a neighbor relationship is established.

    PSNPs are also used for LSDB synchronization.

- IS-IS supported type-length-value (TLV) types

  IS-IS supports 26 types of TLV.

  Table 1 lists IS-IS supported TLV types.

Table 1-1 IS-IS Supported TLV Types

TLV Code	Description
Code=1	Area address
Code=2	Priority of an IS-IS neighbor
Code =3	ES neighbor
Code=6	MAC address of an IS-S neighbor
Code=8	Padded field
Code=9	LSP entity
Code=10	Verification field

TLV Code	Description
Code=14	Size of the source LSP buffer
Code=22	Extended IS reachability
Code=128	IP internal reachability information
Code=129	Supported protocol
Code =130	IP external reachability information
Code=131	Inter-domain routing protocol information
Code=132	IP interface address
Code=133	Verification information
Code=135	Extended IP reachability TLV
Code=137	Dynamic host name
Code = 211	Graceful Restart
Code = 222	MT IS TLV
Code = 229	Multi Topology TLV
Code=232	IPv6 interface
Code = 235	IPv4 MT IP reachability TLV
Code =236	IPv6 IP reachability TLV
Code = 237	IPv6 MT IP reachability TLV
Code =240	P2P three-way handshake TLV

- IS-IS supported network types

  IS-IS supported network types include P2P links and broadcast links.

2. Working Process of IS-IS

IS-IS working process consists of neighbor establishment, LSDB synchronization, and route computation. In a broadcast network, neighbor establishment involves DIS election.

- Neighbor establishment

  The IS-IS neighbor establishment procedure is similar to the OSPF neighbor establishment procedure. If the received hello packets do not contain any information, the neighbor state is reset to Initial. If the neighbor field in the received packets indicates the local MAC address, the neighbor state is Up. If the neighbor state of the local router and peer routers is Up, the neighbor relationship is successfully established.

- DIS election

  A DIS in a broadcast network works like a DR in OSPF.

A pseudonode is generated by a DIS and sets up a relationship with each device in the local network.

Like DR election in OSPF, a DIS is elected to reduce unnecessary neighbor relationships and route information exchanges. After neighbor establishment, the DIS election starts at respective levels of areas. The election priority also changes with the levels of areas.

A DIS simulates multiple access links as a pseudonode and generates LSPs for the pseudonode. The pseudonode sets up a relationship with each device in the local network and forbids direct communication between the devices. A broadcast subnet and a non-broadcast multiple access (NBMA) network are considered as pseudonodes externally. Non-DIS devices report local link states to the DIS in the same network, and the DIS reports the link states on behalf of all the IS devices in the network.

DIS election in IS-IS is preemptive. The election result can be manually controlled through interface priority configuration. The device with a higher interface priority is more likely to be elected as the DIS. A device with the priority 0 participates in DIS election as well.

- LSDB synchronization

  All devices running link state routing protocols send local link state and directly-connected network link state to neighbors. Upon receiving the link information, the neighbors record and forward the information to their neighbors. After link state update is completed, all routers obtain topological information of the entire network. This is referred to as LSDB flooding synchronization.

  Many neighbor actions such as neighbor or neighbor interface up/down, metric change, redistributed route change and periodic change, trigger LSDB synchronization.

  A router processes a received LSP as follows:

  a The router searches for this LSP in the LSDB. If the LSP does not exist in the LSDB, the router records this packet in the LSDB and broadcasts it for synchronization.

  b If the sequence number of this LSP is greater than that of the local LSP, the router updates the LSDB and broadcasts it for synchronization.

  c If the sequence number of this LSP is smaller than that of the local DPS, the router replies to the local LSP.

- Route computation

  After the LSDB is synchronized, IS-IS computes the SPF and generates IS-IS routes based on the SPF.

  In the LSP sent by the Level-1/Level-2 routers, ATT is set to 1. A Level-1 router gets to know the closest Level-1/Level-2 router based on the ATT and route computation result, and considers the Level-1/Level-2 router a routing transit to other areas.

3. IS-IS Route Control

- Route redistribution

  IS-IS can introduce routes of other routing protocols and routes of other IS-IS processes to the IS-IS process and mutually introduce routes between Level-1 and Level-2 areas.

  In IS-IS, a Level-2 area does not synchronize the known routing information of the backbone areas and other Level-1 areas to a Level-1 area. The Level-2 area cannot obtain external routing information outside Level-1 area. During routing, secondary routes may be generated. During route redistribution, routes of other Level-1 areas and backbone areas that meet conditions can be introduced to the local Level-1 area based on the routing policy.

- Route summarization

  Route summarization is a process of summarizing routing information with the same prefix into one route, and advertising the summarized route (replacing a large number of individual routes) to neighbors. Route summarization helps reduce the protocol interaction load, the size of the routing table, and the impact of route flapping on the routing table.

- Load balancing

  If multiple equal-cost routes exist in a network, IS-IS can distribute load to the equal-cost routes to improve link usage.

4. IS-IS Wide Metric

The default metric type of IS-IS is narrow. In narrow mode, the maximum metric value of an interface is **63**. In a large network, the metric value range in narrow mode is not wide enough. Therefore, wide metric is developed. The metric value can reach 16777215.

5. LSP Fragment Extension

IS-IS advertises link state information by flooding LSPs. The size of an LSP is limited by the MTU size of the link. When the content to be advertised exceeds one LSP, IS-IS will create LSP fragments to carry new link state information. Based on ISO, an LSP fragment is indicated by an LSP number that is one byte long. Therefore, an IS-IS device can generate a maximum of 256 LSP fragments.

The 256 LSP fragments are insufficient in any of the following situations:

(1) New applications (such as traffic engineering) extend new TLV or sub-TLV.

(2) The network is expanded continuously.

(3) Routes with reduced granularity are advertised, or other routes are redistributed to IS-IS.

After LSP fragments are used up, new routing information and neighbor information will be discarded, causing network exceptions such as routing black holes or loops. To ensure normal network operation, LSP fragments must be extended to carry more link state information.

By configuration of an additional system ID and an fragment extension switch, IS-IS can advertise more link state information in extended LSP fragments. Each virtual system can be considered as a virtual device that establishes a neighbor relationship (with the path value 0) with the originating system. Extended LSPs are advertised by the neighbor of the originating system, that is, the virtual system.

The following terms are related to fragment extension:

- Normal system ID

  The system ID defined by ISO is used to establish neighbor relationships and learn routes. It is further defined as the normal system ID in order to be distinguished from the additional system ID introduced to fragment extension.

- Additional system ID

  The additional system ID is configured by an administrator to generate extended LSPs. The additional system ID shares the usage rules of the normal system ID (for example, the additional system ID must be unique in the entire area), except that the additional system ID is not carried in Hello packets for neighbor relationship establishment.

- Originating system

An originating system is an IS-IS-enabled device and maps to a virtual system identified by the additional system ID.

- Virtual system

  A virtual system is identified by the additional system ID and used to generate extended LSPs. The concept of virtual system is proposed by RFC for distinguishing from the concept of originating system. Each virtual system can generate up to 256 LSP fragments. The administrator can configure multiple additional system IDs (virtual systems) to generate more LSP fragments.

- Original LSP

  An original LSP is the LSP whose system ID contained in the LSP ID is a normal system ID. Original LSPs are generated by an originating system.

- Extended LSP

  An extended LSP is the LSP whose system ID contained in the LSP ID is an additional system ID. Extended LSPs are generated by a virtual system.

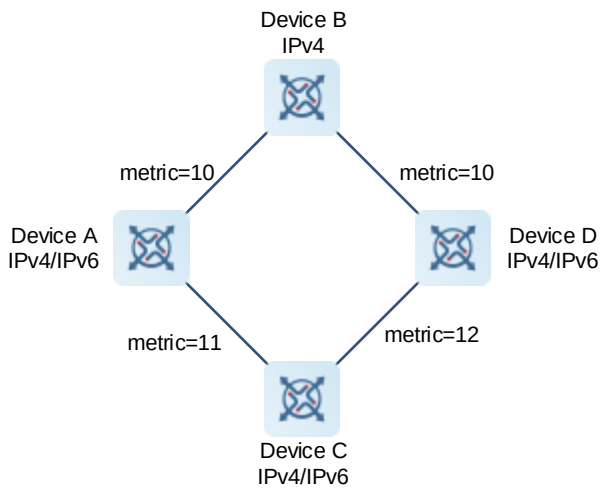
6. IS-IS MTR

IS-IS multi-topology routing (MTR) is an extended feature used to separate IPv4 unicast route computation from IPv6 unicast route computation based on topologies. New TLV types introduced to IIH packets and LSP packets of IS-IS to transmit IPv6 unicast topology information. One physical network can be divided into an IPv4 unicast logical topology and an IPv6 unicast logical topology. The two topologies perform SPF computation separately and maintain respective independent IPv4 and IPv6 unicast routing tables. In this way, IPv4 unicast service traffic and IPv6 unicast service traffic are forwarded by different paths. The IS-IS MTR technique helps users deploy IPv6 unicast networks without the constraint on consistency between IPv4 and IPv6 unicast topology information.

IS-IS MTR is derived from IS-IS MT, which is used to separate IPv4 unicast topology from IPv6 unicast topology, unicast topology from multicast topology, and topologies using different protocol stacks (such as IPv4 and Pv6). IS-IS MTR separates IPv4 unicast topology from IPv6 unicast topology based on IS-IS MT.

Figure 1-3 shows a typical networking application with the following implementation requirements: Deploy an IPv6 unicast topology in incremental mode and upgrade some devices to support IPv4 and IPv6 dual protocol stacks while keeping other IPv4-enabled devices unchanged.

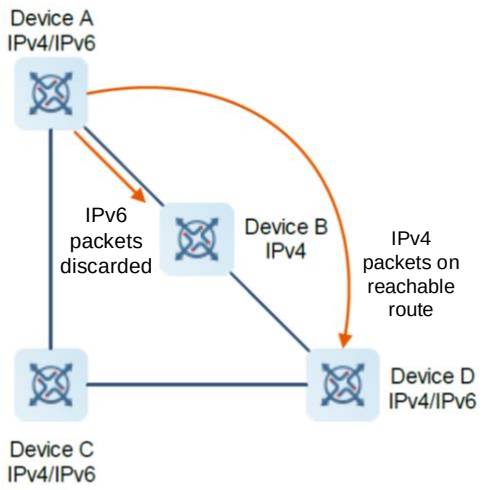
Figure 1-3 Physical Topology for IPv4/IPv6 Hybrid Deployment



As shown in Figure 1-3, each link is marked by a number indicating its metric. Device B only supports the IPv4 protocol stack, whereas other devices support IPv4 and IPv6 dual protocol stacks.

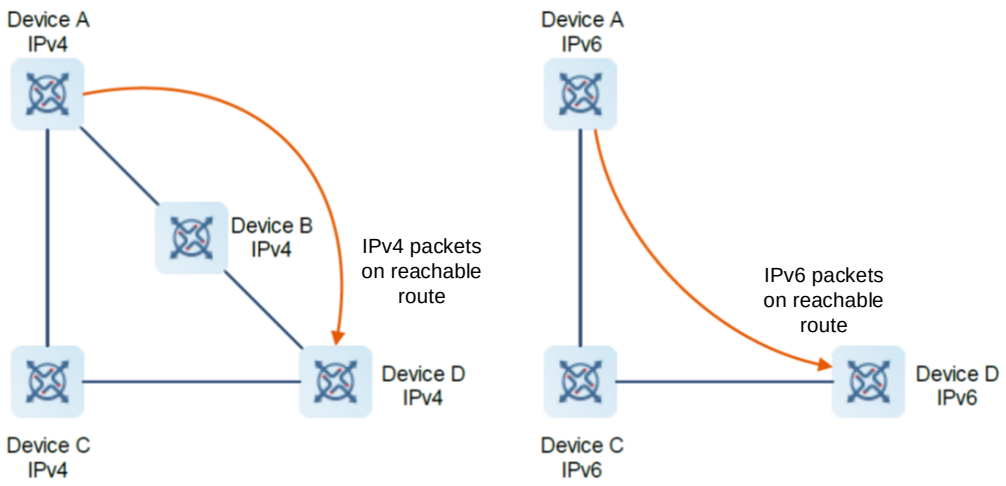
The networking constraint on consistency between IPv4 and IPv6 unicast topologies must be removed to retain the use of Device B (supporting IPv4) so that Device B can establish a neighbor relationship with Device A or D. This, however, may cause new problems.

Figure 1-4 IPv4/IPv6 Hybrid Topology



As shown in Figure 1-4, without IS-IS MTR, SPF computation performed by Devices A, B, C, and D only take into account the single hybrid topology. The calculated shortest path is Device A -> Device B -> Device D, with the cost 20. Device B will discard IPv6 packets because it does not support IPv6.

Figure 1-5 Separation of IPv4 and IPv6 Topologies



As shown in Figure 1-5, after the IS-IS MTR technique is used to separate IPv4 unicast topology from IPv6 unicast topology, Devices A, B, C, and D establish neighbor relationships based on the IPv4 and IPv6 unicast topologies. The left part shows the IPv4 topology formed by IPv4-enabled routers. The calculated IPv4 shortest

path is Device A -> Device B -> Device C, which realizes IPv4 packet forwarding. The right part shows the IPv6 topology formed by IPv6-enabled routers. The calculated IPv6 shortest path is Device A -> Device C -> Device D, which realizes IPv6 packet forwarding.

General IS-IS MTR deployment: IS-IS MTR must be deployed to avoid routing black holes when some devices support only one protocol. IS-IS MTR is not required when all devices support IPv4 and IPv6 dual protocol stacks.

Deployment of a new network: IS-IS MTR is not required when devices only support the IPv4 protocol stack. For devices that only support the IPv6 protocol stack or devices that support IPv4 and IPv6 dual protocol stacks, enable the MT mode of IS-IS MTR. You are not advised to enable Multi-Topology Transition (MTT) because loops may occur.

Reconstruction of an existing network with devices supporting only one protocol stack: Enable the MTT mode of IS-IS MTR on devices that support IPv4 and IPv6 dual protocol stacks in sequence (starting from the device closest to a device supporting only one protocol stack in the network topology). After the MTT mode is enabled on all new devices, switch the MTT mode to the MT mode on these devices in sequence (starting from the device farthest from a device supporting only one protocol stack in the network topology).

7. IS-IS Neighbor

In a broadcast network, neighbors elect a DIS and routers send routing information to the DIS.

On a P2P link, neighbor relationship can be established in two ways:

- Two-way handshake

  As long as an IIH packet is received, neighbor relationship is established. This method comes with low reliability.

- Three-way handshake

  Neighbor relationship can be established after the IIH packet is sent three times. This method boasts high reliability.

  In a link with one down end, if a neighbor relationship is established based on the IIH packet received from the peer device, the established neighbor relationship is abnormal. In a three-way handshake, an acknowledgment packet must be received from the peer device to confirm that the peer device has received the IIH packet before the neighbor relationship is established.

The following conditions must be met for two routing devices to establish a neighbor relationship when IS-IS MTR is not configured:

- The interface addresses on both routing devices are in the same network segment.
- The interface levels on both routing devices match.
- The routing devices are authenticated by each other.
- The routing devices support the same protocol.

The following conditions must be met for two routing devices to establish a neighbor relationship when IS-IS MTR is configured:

- The interface addresses on both routing devices are in the same network segment.
- The interface levels on both routing devices match.
- The routing devices are authenticated by each other.
- The routing devices have at least one consistent MT ID when P2P links are configured.

- There are no constraints on the MT IDs that the routing devices support when LAN links are configured.

8. IS-IS Authentication

Internet requirements for information security increase. To avoid data theft and tampering, operators apply the IS-IS authentication function on specified areas or interfaces to ensure data security.

- IS-IS authentication types

  Classification based on packet types:

  - Interface authentication: Authenticate Level-1 and Level-2 hello packets.
  - Area authentication: Authenticate Level-1 CSNP, PSNP, and LSP packets.
  - Routing domain authentication: Authenticate Level-2 CSNP, PSNP, and LSP packets.

  Classification based on authentication mode:

  - Simple authentication: Add a configured password to a packet. This authentication mode comes with low security.
  - MD5 authentication: A password is encrypted using MD5 algorithms and then added to a packet.
  - Keychain authentication: A keychain is configured so that the password changes with time.

- Implementation procedure

  Upon receiving an IS-IS packet from another router, the local router checks whether the authentication password is correct. If not, the packet is discarded. The IS-IS packet carries authentication information by means of TLV. The TLV format is as follows:

  - Type: Indicates an authentication packet type. For TCP/IP packets, this value is 133.
  - Length: Indicates the length of a TLV.
  - Value: Indicates an authentication type and password.

  Interface authentication: Indicates that authentication is configured in interface configuration mode. Interconnected router interfaces must be configured with the same password.

  Area authentication: Indicates that authentication is configured in IS-IS routing process configuration mode. If the authentication is performed between routers in the same area, the key string or password must be the same.

  Routing domain authentication: Indicates that authentication is configured in IS-IS routing process configuration mode. If the authentication is performed between routers in the same routing domain, the key string or password must be the same.

  SNP packets can be authenticated separately from LSP packets and authentication check can be enabled for the received LSP or SNP packets.

9. IS-IS GR

For GR to be successful, the following two conditions must be met:

- The network topology is stable.
- The device can ensure uninterrupted forwarding when it restarts IS-IS.

Two roles exist during the GR process: Restarter and Helper. Accordingly, the IS-IS GR function is divided into IS-IS GR Restart and IS-IS GR Help capabilities. A device with the IS-IS GR Restart capability can send GR requests and automatically execute GR. A device with the IS-IS GR Help capability can receive GR requests

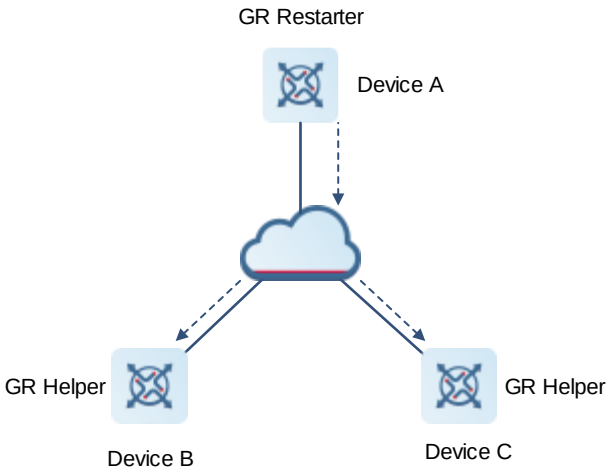
and assist neighbors in executing GR. The GR process starts when the Restarter sends a GR request. After receiving the GR request, the neighboring device enters Help mode to help the Restarter reestablish its LSDB while maintaining the neighbor relationship with the Restarter.

When an IS-IS device performs GR, it notifies its neighbors to maintain their neighbor relationship so that other devices in the network cannot sense the change in the topological relationship and the neighbors will not recalculate the route and update its forwarding table. The IS-IS device synchronizes and restores the LSDB to its pre-GR state with the help of the neighbors to ensure that the routing table and forwarding table remain unchanged before and after GR implementation and data forwarding is not interrupted.

The Restarter performs the following operations during the GR process:

(1) The GR Restarter notifies the GR Helpers that the local device will be restarted.

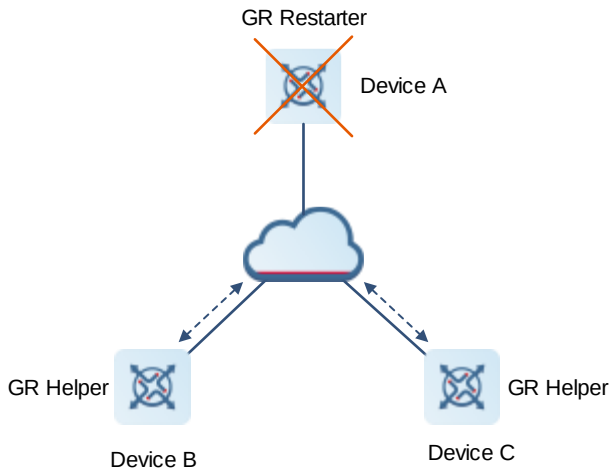
Figure 1-6 Restarter Notifying Helpers of GR



Device A acts as the GR Restarter, and Devices B and C are GR Helpers of Device A. Device A sends a GR request instructing all its neighbors not to delete the neighbor relationships with Device A when it is restarted. After receiving the GR request, the neighbors send GR responses to the GR Restarter, and maintain their neighbor relationships with the GR Restarter during the GR time (specified by GR grace-period) notified by the GR Restarter.

(2) The GR Restarter is restarted.

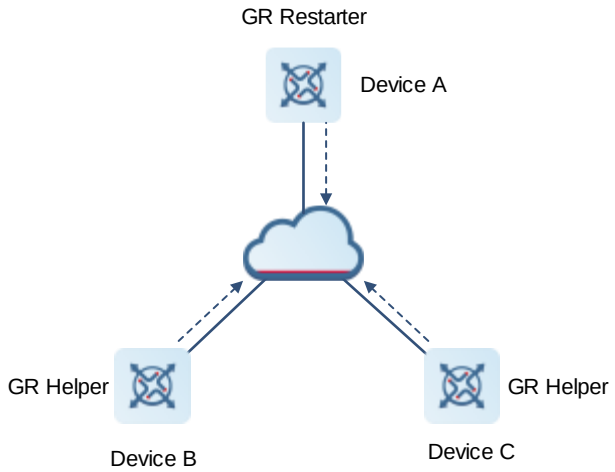
Figure 1-7 Restarter Restart



When the GR Restarter is restarted, its IS-IS interface changes from down state to up state. The GR Helpers know that the GR Restarter is in IS-IS restart state, they maintain their neighbor relationships with the GR Restarter during the GR time and retain the routes from the GR Restarter.

(3) The GR Restarter synchronizes topology and routing information from the GR Helpers.

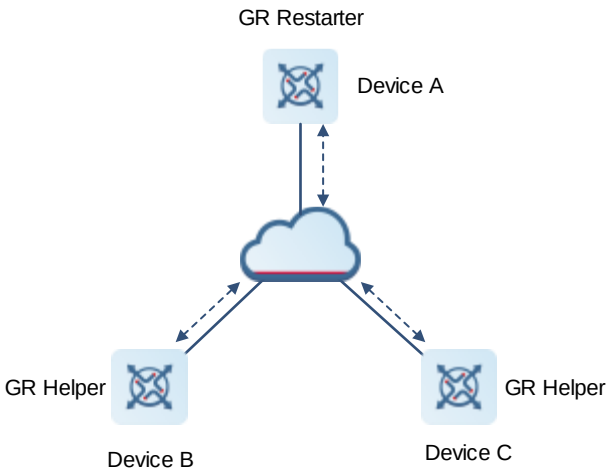
Figure 1-8 LSDB Synchronization



After IS-IS restart, the GR Restarter synchronizes topology or routing information from the GR Helpers and recalculates its routing table. During the process, any change in the routing table is not updated to the forwarding table.

(4) GR is completed when the GR Restarter finishes LSDB synchronization. Then all devices enter IS-IS interaction state.

Figure 1-9 GR Completion



After the GR Restarter synchronizes all required data, all devices enter IS-IS interaction state. The routing table of the GR Restarter is updated to the forwarding table and invalid entries are cleared. Because the GR Restarter is completely restored to the pre-restart state under stable network conditions, its routing table and forwarding table remain unchanged before and after GR.

10. Fast Convergence of IS-IS

IS-IS accelerates convergence by fast advertisement of LSPs and smart timer.

- Fast advertisement of LSPs

  By modification of LSP flooding interval and maximum number of LSPs sent on an interface, LSPs can be advertised to the IS-IS area in the route computation time to reduce route computation and accelerate convergence when the LSPs trigger route computation.

- Smart timer

  LSP packet generation time and SPF algorithm computation time are adjusted based on the smart timer. In a stable IS-IS network, the route computation frequency is low and the first SPF algorithm time is short. In a network with ever-changing topology and network jitter, route computation frequency increases, which consumes CPU resources. In this case, the smart timer will increase SPF computation delay to accelerate convergence and reduce CPU consumption.

1.1.3 Protocols and Standards

- RFC 1142: OSI IS-IS Intra-domain Routing Protocol
- RFC 1195: Use of OSI IS-IS for routing in TCP/IP and dual environments
- RFC 3786: Extending the Number of Intermediate System to Intermediate System (IS-IS) Link State PDU (LSP) Fragments Beyond the 256 Limit
- RFC 3373: Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- RFC 3358: Optional Checksums in Intermediate System to Intermediate System (ISIS)
- RFC 3784: Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
- RFC 2763: Dynamic Hostname Exchange Mechanism for IS-IS

- RFC 6119(draft-ietf-isis-ipv6-te-00): IPv6 Traffic Engineering in IS-IS
- RFC 2966: Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 5306: Restart Signaling for IS-IS

1.2 Restrictions and Guidelines

The PIM mode enabled on all interfaces of a device for an instance must be consistent.

1.3 Configuration Task Summary

IS-IS configuration includes the following tasks:

(1) Configuring Basic Settings of IS-IS

(2) (Optional) Configuring IS-IS network Levels

(3) (Optional) Configuring IS-IS Hello Packets

(4) (Optional) Configuring IS-IS LSPs

(5) (Optional) Configuring IS-IS SNPs

(6) (Optional) Configuring IS-IS Route Advertisement

(7) (Optional) Configuring IS-IS Route Summarization

(8) (Optional) Configuring an IS-IS Passive Interface

(9) (Optional) Controlling IS-IS Routing Factors

(10) (Optional) Configuring the Priority of an IS-IS Device

(11) (Optional) Configuring IS-IS Authentication

(12) (Optional) Configuring IS-IS GR

(13) (Optional) Configuring IS-IS NSR

(14) (Optional) Correlating IS-IS with BFD

(15) (Optional) Configuring the IS-IS Overload Bit

(16) (Optional) Configuring IS-IS VRF

(17) (Optional) Configuring IS-IS MTR

(18) (Optional) Configuring IS-IS SNMP

(19) (Optional) Enabling Super VLAN for IS-IS

(20) (Optional) Configuring IS-IS Two-way Maintenance

(21) (Optional) Configuring Extended Feature of IS-IS

The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring the Maximum Metric of a Neighbor
- Configuring the Maximum Number of Area Addresses
- Configuring SPF Calculation Interval
- Canceling Three-Way Handshake of a P2P Network
- Enabling TLV to Be Padded Based on Supported Protocol

- Configuring the Reachable Time of a Suppressed Neighbor
- Enabling Adjacency Event Output

1.4 Configuring Basic Settings of IS-IS

1.4.1 Overview

Basic settings of IS-IS are a precondition for configuration of all IS-IS features and basic internetworking.

1.4.2 Restrictions and Guidelines

- The Level-1 IS-IS devices in an area must be configured with the same area ID.
- The core routing table does not distinguish the routing entries generated by different IS-IS routing processes.
- The IP addresses of interfaces connected between neighbors must be in the same network segment.
- If the IP addresses are in different network segments, a neighbor relationship cannot be established.
- If you need to add an interface to the specified IS-IS routing process and configure the interface with the IPv4 IS-IS function, add the tag parameter after the **ip router isis** command to indicate the process name.
- If you run the **no ip routing** command in global configuration mode, IS-IS will disable IPv4 routing on all interfaces. That is, the **no ip router isis** *[tag]* command is automatically executed on all interfaces, with other IS-IS settings unchanged.
- If you need to add an interface to the specified IS-IS routing process and configure the interface with the IPv6 IS-IS function, add the tag parameter after the **ipv6 router isis** command to indicate the process name.
- If you run the **no ipv6 unicast-routing** command in global configuration mode, IS-IS will disable IPv6 routing on all interfaces. That is, the **no IPv6 router isis** *[tag]* command is automatically executed on all interfaces, with other IS-IS settings unchanged.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IS-IS routing process and enter the IS-IS routing process configuration mode.

router isis [*tag*]

No IS-IS instance is configured by default.

If you configure the *tag* parameter when you start an IS-IS routing process, you need to add this tag parameter when you stop the IS-IS routing process.

(4) Configure a NET address in IS-IS.

net *net-address*

No NET address is configured in IS-IS by default.

Different NET addresses must have the same system ID.

(5) (Optional) Modify the system ID in IS-IS. Configure one of the following tasks.

- Replace the system ID of an instance with the configured name.

  is-name *name*

  The default system ID is used.

- Replace the system ID of a router with the host name of the destination router.

  hostname dynamic

  The host name replacement function is enabled by default.

(6) Return to the global configuration mode.

exit

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Enable IS-IS on an interface.

- Enable IPv4 IS-IS on an interface.

  ip router isis [*tag*]

  IPv4 IS-IS is not enabled on an interface by default.

- Enable IPv6 IS-IS on an interface.

  ipv6 router isis [*tag*]

  IPv6 IS-IS is not enabled on an interface by default.

1.5 Configuring IS-IS network Levels

1.5.1 Overview

IS-IS supports a two-Level system to realize routing management and extensible route selection in a large network. Each level is only concerned about maintaining the topology of the corresponding area.

1.5.2 Restrictions and Guidelines

- If the circuit-type is set to Level-1 or Level-2-only, IS-IS will only send PDUs at the corresponding level.
- If the circuit type of an interface is set to **external**, this interface will work as an external domain interface and IS-IS will not send PDUs at the corresponding level.
- A device can have only one instance running at Level-2 (including Level-1/Level-2).

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Configure a level of IS-IS.

is-type { **level-1 | level-1-2 | level-2-only** }

IS-IS runs at Level-1/Level-2 by default.

(5) Return to the global configuration mode.

exit

(6) Enter the interface configuration mode.

interface *interface-type interface-number*

(7) Configure an IS-IS level on an interface.

isis circuit-type { **level-1 | level-1-2 | level-2-only** [**external**] }

The circuit type of an interface is set to Level-1/Level-2 by default.

(8) Configure a broadcast interface as a P2P interface.

isis network point-to-point

The broadcast network type is unchanged by default.

1.6 Configuring IS-IS Hello Packets

1.6.1 Overview

Hello packet control parameters, including hello packet sending interval, hello holdtime, packet padding, and neighbor detection are configured. Neighbor establishment can be controlled to maintain neighbor interaction.

1.6.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the Hello packet sending interval of an interface.

isis hello-interval { *interval* | **minimal** } [**level-1 | level-2**]

The Level-1 and Level-2 hello packets are sent at an interval of **10** seconds by default.

(5) Configure the Hello packet holdtime multiplier on an interface.

isis hello-multiplier *multiplier-number* [**level-1** | **level-2**]

The default hello holdtime multiplier is **3**. That is, the hello holdtime is three times of the hello interval.

(6) Configure to pad IS-IS hello packets on an interface.

isis hello padding

Padding is enabled by default for hello packets sent on an interface.

(7) Enable neighbor supported protocol detection for hello packets in IPv4 environment.

adjacency-check

The neighbor supported protocol detection function for hello packets is enabled by default.

(8) Enter the IS-IS IPv6 address family configuration mode.

address-family ipv6 unicast

(9) Enable neighbor supported protocol detection for hello packets in IPv6 environment.

adjacency-check

The neighbor supported protocol detection function for hello packets is enabled by default.

(10) Exit the IS-IS IPv6 address family configuration mode.

exit-address-family

1.7 Configuring IS-IS LSPs

1.7.1 Overview

Adjusting timer and packet length of LSPs will affect LSP update timeliness and LSP frequency.

1.7.2 Restrictions and Guidelines

- The LSP generation time and refresh time can be configured to prevent network topology change from affecting the LSP transmission frequency.
- During LSDB change, IS-IS notifies the change by LSP advertisement. If a great number of IS-IS routes and interfaces exist on a device, a too small sending interval and a too great LSP number may cause LSP bursts. Therefore, the LSP sending interval and LSP number must be set to proper values. LSP retransmission interval is used in P2P network. In such a network, an LSP response must be returned to indicate completion of an LSP retransmission.
- The value of *lsp-refresh-interval* must be smaller than that of *max-lsp-lifetime*.
- The value of *max-lsp-lifetime* must be greater than that of *lsp-refresh-interval*.
- The value of the configured *initial-interval* cannot be greater than that of *maximum-interval*. Otherwise, the value of *initial-interval* is changed to that of *maximum-interval*.
- The value of the configured *hold-interval* cannot be greater than that of *maximum-interval*. Otherwise, the value of *hold-interval* is changed to that of *maximum-interval*.
- The value of the configured *initial-interval* cannot be greater than that of *hold-interval*. Otherwise, the value of *initial-interval* is changed to that of *hold-interval*.
- If no particular level is specified in the command, the default level is Level-1/Level-2, which means that the interval configuration takes effect to Level-1 and Level-2 concurrently.
- When you need to configure **mesh-group** on an IS-IS interface, run the **isis csnp-interval** command to configure the non-0 CSNP interval to ensure complete LSP synchronization between neighbors in the network. After that, CNSPs will be periodically sent to synchronize LSPs.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Modify LSP control parameters on the interface. The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configure the LSP sending interval.

  isis lsp-interval *interval* [**level-1** | **level-2**]

  LSPs are sent at an interval of **33** ms by default on an IS-IS interface.

- Configure the maximum number of LSPs sent by an IS-IS interface at a time.

  isis lsp-flood *lsp-number* [**level-1** | **level-2**]

  An IS-IS interface sends at most 5 LSPs at a time by default.

- Configure the LSP retransmission interval.

  isis retransmit-interval *retransmit-interval* [**level**-1 | **level**-2]

  LSPs are retransmitted at an interval of **5** seconds by default.

  If *retransmit-interval* is set to **0**, no LSP is retransmitted.

(5) Return to the global configuration mode.

exit

(6) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(7) Modify LSP control parameters in the IS-IS process. The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configure the LSP generation interval.

  lsp-gen-interval [**level-1** | **level-2**] *maximum-interval* [*initial-interval hold-interval*]

  The default maximum interval between two LSP generation times is **5** seconds, the delay for generating an LSP is **50** ms, and the minimum interval between the first LSP generation time and the second LSP generation time is **200** ms.

- Configure the LSP refresh interval.

  lsp-refresh-interval *interval*

  The default LSP refresh interval is **900** seconds.

- Configure the LSP lifetime.

  max-lsp-lifetime *max-lifetime*

  The default maximum LSP lifetime is **1200** seconds.

- Configure the interval for receiving duplicate LSP packets.

  min-lsp-arrival [**level-1** | **level-2**] *minimum-interval initial-interval hold-interval*

  The function of receiving duplicate LSP packets is not supported by default.

- Configure to ignore LSP checksum errors.

  ignore-lsp-errors

  LSP checksum errors are processed by default.

- Configure LSP fragment extension.

  lsp-fragments-extend [**level-1** | **level-2**] [**compatible rfc3786**]

  The fragment extension function is disabled by default. To enable fragment extension, run this command to configure fragment extension at the specified level and run the **virtual-system** command to configure an additional system ID.

- Configure the additional system ID of the IS-IS routing process.

  virtual-system *system-id*

  No additional system ID is configured by default. To enable fragment extension, run this command to configure an additional system ID and run the **lsp-fragments-extend** command to configure fragment extension.

- Configure the maximum length of received LSPs.

  lsp-length receive *size*

  The default maximum length of received LSPs is **1492** bytes.

- Configure the maximum length of sent LSPs.

  lsp-length originate *size* [**level-1** | **level-2**]

  The default maximum length of sent LSPs is **1492** bytes.

- Add an IS-IS interface to a specified mesh group.

  isis mesh-group { **blocked** | *mesh-group-id* }

  No interface joins any mesh group by default.

1.8 Configuring IS-IS SNPs

1.8.1 Overview

By default, a DIS in a broadcast network sends a CSNP every 10s for LSDB synchronization. In a P2P network, CSNPs are sent only after a neighbor relationship is established.

1.8.2 Restrictions and Guidelines

- If an interface is added to a mesh group, CSNP sending interval can be configured. If the CSNP interval is set to **0**, no CSNP is sent.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the CSNP broadcast interval on an IS-IS interface.

isis csnp-interval *interval* [**level-1** | **level-2**]

CSNPs are sent at an interval of **10** seconds in a broadcast network by default. No CSNPs are sent in a P2P network by default.

When you configure a new CSNP interval without specifying Level-1 or Level-2, the interval configuration takes effect for Level-1 and Level-2 CSNPs by default.

(5) Configure the minimum PSNP sending interval.

isis psnp-interval *psnp-interval* [**level-1** | **level-2**]

The function of configuring the PSNP sending interval is disabled by default. In this case, the minimum PSNP sending interval is **2** seconds by default and it takes effect for Level-1 and Level-2 PSNPs.

1.9 Configuring IS-IS Route Advertisement

1.9.1 Overview

IS-IS can introduce routes of other routing protocols and routes of other IS-IS processes to the IS-IS process and mutually introduce routes between Level-1 and Level-2 areas.

1.9.2 Restrictions and Guidelines

- Because Level-2 domains do not generate any default route, the **default-information originate** command is run to allow a default route to enter a Level-2 domain.
- In the old versions of some vendors, if **metric-type** is set to **external**, the metric of redistributed routes is added by 64 during route calculation and used to determine routing. This practice does not comply with the related protocol. In the actual application, external routes may be preferred over internal routes. If this happens during interworking with old versions of some vendors, you can modify the related setting (such as **metric** or **metric-type**) of each device to ensure that internal routes are preferred over external routes.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Generate a default route.

default-information originate [**route-map** *map-name*]

No default route is generated by default.

(5) Redistribute other routes to IS-IS.

redistribute { **bgp** | **connected** | **ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] } *] | **rip** | **static** } [[**level**-1 | **level**-1-2 | **level**-2] | **metric** *metric-value* | **metric-type** { **external** | **internal** } | **route-map** *route-map-name*] *

Redistribution is disabled by default.

(6) Redistribute the Level-1 reachable routing information of the specified IS-IS instance to Level-2 of the current instance.

redistribute isis [*tag*] **level-1 into level-2** [**distribute-list** *acl-name* | **route-map** *route-map-name*]

Redistribution is disabled by default.

(7) Redistribute the Level-2 reachable routing information of the specified IS-IS instance to Level-1 of the current instance.

redistribute isis [*tag*] **level-2 into level-1** [**distribute-list** *acl-name* | {

ipv6-prefix *ipv6-address/length* |

prefix *ipv4-address net-mask* } | **route-map** *route-map-name*]

Redistribution is disabled by default.

1.10 Configuring IS-IS Route Summarization

1.10.1 Overview

Configuring route summarization can effectively reduce the size of a routing table and system resource usage. If the links in the range of the IP addresses to be summarized jitter (up and down), advertisement of the summarized routes is not affected to avoid route flapping. After route summarization, if any routing information about a reachable address or network segment exists, a summarized route, instead of a detailed route, is advertised externally.

1.10.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Configure an IPv4 summarized route.

summary-address *ipv4-address net-mask* [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value*]

The route summarization function is disabled by default.

(5) Enter the IS-IS IPv6 address family configuration mode.

address-family ipv6 unicast

(6) Enable IPv6 route summarization.

summary-prefix *ipv6-prefix/prefix-length* [**level-1** | **level-1-2** | **level-2**]

The route summarization function is disabled by default.

1.11 Configuring an IS-IS Passive Interface

1.11.1 Overview

This function prevents the specified interface from receiving and sending IS-IS packets, but the IP address of this interface will be flooded by other interfaces.

1.11.2 Restrictions and Guidelines

- If the number of interfaces with IS-IS not enabled exceeds 255, only the first 255 interfaces will be configured as passive interfaces. The remaining interfaces are non-passive interfaces.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Configure a passive interface in the IS-IS routing process configuration mode.

passive-interface { **default** | *interface-type interface-number* }

The passive interface function is disabled by default.

(5) Return to the global configuration mode.

exit

(6) Enter the interface configuration mode.

interface *interface-type interface-number*

(7) Configure a passive interface.

isis passive

The configured passive interface in the IS-IS routing process configuration mode prevails by default.

1.12 Controlling IS-IS Routing Factors

1.12.1 Overview

IS-IS routing is determined by adjusting the number of equal-cost routes, reference bandwidth values, and interface costs.

1.12.2 Restrictions and Guidelines

- The **maximum-paths** command is used by IS-IS to control the number of IS-IS equal-cost paths to be added to a routing table. There is also a routing table command used to control the number of equal-cost paths. The number of effective equal-cost paths is determined by either of the two command values, whichever is smaller.

- The **bandwidth-reference** command is used to calculate the interface metric in an instance based on the bandwidth value configured in the instance. If a metric is configured, the metric prevails.
- The metric, which is used in SPF calculation, is stored in the IP reachability information TLV. A greater metric value indicates a greater routing consumption of this interface and a longer path of SPF calculation. The Narrow-metric value is valid only when Metric-style is set to **Narrow**. The Wide-metric value is valid only when Metric-style is set to **Wide**.

1.12.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Configure the administrative distance of an IS-IS route.

distance *distance-value*

The default administrative distance of IS-IS is **115**.

(5) Configure the maximum number of equal-cost paths.

maximum-paths *maximum*

The default maximum number of equal-cost paths is **2**.

(6) Configure the reference bandwidth value for cost computation.

bandwidth-reference *value*

The default reference bandwidth value for cost computation is **100** Mbps.

(7) Configure the metric type.

metric-style { **narrow** | **wide** } [**transition**] [**level-1** | **level-2** | **level-1-2**]

The default metric type is Narrow.

(8) Return to the global configuration mode.

exit

(9) Enter the interface configuration mode.

interface *interface-type interface-number*

(10) Configure metric of the IS-IS interface.

isis metric *metric* [**level-1 | level-2**]

Level-1 and Level-2 use the computation result of bandwidth-reference by default.

(11) Configure the wide metric value of an interface.

isis wide-metric *metric* [**level-1 | level-2**]

The default wide metric value of Level-1 and Level-2 is the computation result of **bandwidth-reference**.

1.13 Configuring the Priority of an IS-IS Device

1.13.1 Overview

Adjusting DIS election priority of a device on an interface can manually affect DIS election result and specify a device to become the DIS.

1.13.2 Restrictions and Guidelines

- A lower DIS priority of an interface indicates a lower priority of being elected as a DIS.
- This function is invalid on a P2P network interface.

1.13.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure device priority in DIS election.

isis priority *value* [**level-1 | level-2**]

The default priority of a device for Level-1 and Level-2 DIS election is **64**.

1.14 Configuring IS-IS Authentication

1.14.1 Overview

Internet requirements for information security increase. To avoid data theft and tampering, operators apply the IS-IS authentication function on specified areas or interfaces to ensure data security.

- Interface authentication is intended for establishing and maintaining neighbor relationships. A neighbor relationship cannot be established between two IS-IS devices with different interface authentication passwords. This prevents unauthorized or unauthenticated IS-IS devices from joining an IS-IS network that requires authentication. Interface authentication passwords are encapsulated in Hello packets before being sent.
- Area authentication and routing domain authentication in IS-IS are performed to verify LSPs, CSNPs, and PSNPs to prevent unauthorized or unauthenticated routing information from being injected into the LSDB. Authentication passwords are encapsulated in LSPs, CSNPs, and PSNPs before being sent.

1.14.2 Restrictions and Guidelines

- An interface authentication password is encapsulated in a Hello packet before being sent by an interface. When an interface receives a Hello packet, it checks the password in the packet against the existing one.
- Area authentication passwords are encapsulated in Level-1 LSPs, CSNPs, and PSNPs. When an interface receives an LSP, CSNP, or PSNP, it checks the password in the packet against the existing one.

- Routing domain authentication passwords are encapsulated in Level-2 LSPs, CSNPs, and PSNPs. When an interface receives an LSP, CSNP, or PSNP, it checks the password in the packet against the existing one.
- If no particular Level is specified in the command, the default level is Level-1/Level-2, which means that the authentication configuration takes effect to Level-1 and Level-2 concurrently.
- A key chain may contain multiple passwords. A password with a smaller SN is preferentially used for sending a packet. When the packet arrives at the peer device, the device will receive the packet if the password in the packet is consistent with a password in the key chain.
- For plaintext authentication, the *string-text* in the key chain cannot exceed 80 characters; otherwise, the key chain will be invalid.
- Only one key chain can be used at a time. After you configure a new key chain, it will replace the original one.
- Before you deploy IS-IS interfaces and area authentication on all devices in the network or before you change the authentication password or authentication mode, run the **send-only** command. The devices will not authenticate received Hello packets to avoid network flapping when IS-IS interface authentication is deployed.

1.14.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a key chain, and enter the key chain configuration mode.

key chain *key-chain-name*

(4) Create a key chain, and enter the key chain configuration mode.

key *key-id*

(5) Configure the key.

key-string [**0** | **7**] *string-text*

(6) Exit the key chain configuration mode.

exit

(7) Return to the global configuration mode.

exit

(8) Enter the interface configuration mode.

interface *interface-type interface-number*

(9) Configure Hello packet authentication on an interface.

- Specify the authentication mode as plaintext or MD5.

  isis authentication mode { **md5** | **text** } [**level-1** | **level-2**]

  The interface authentication mode is disabled by default.

  The priority of the password is higher than that of the password configured using the **isis password** command.

- Configure the password for interface authentication.

  isis authentication key-chain *key-chain-name* [**level-1** | **level-2**]

  Authentication is not performed if no key chain is configured using the **key chain** command. In addition to the key chain command, you also need to run the **isis authentication mode** command to make IS-IS key chain authentication take effect.

- (Optional) Configure the password for plaintext authentication of hello packets on an interface.

  isis password [**0** | **7**] *password-string* [**send-only**] [**level-1** | **level-2**]

  Plaintext authentication is not enabled by default.

  This command does not take effect if the **isis authentication mode** command has been run to configure authentication before.

- (Optional) Configure an authentication password in the Hello packets sent. Received Hello packets are not authenticated.

  isis authentication send-only [**level-1** | **level-2**]

  Packets sent and received on an interface are authenticated by default.

(10) Return to the global configuration mode.

exit

(11) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(12) Configure LSP, CSNP, and PSNP packet authentication in an IS-IS area.

- (Optional) Configure a password for plaintext authentication of a Level-1 area.

  area-password [**0** | **7**] *password-string* [**send-only**]

  The plaintext authentication function of a Level-1 area is disabled by default.

  All IS-IS devices in an area must be configured with the same authentication password. This command does not take effect if the **authentication mode** command has been run to configure authentication before.

- (Optional) Configure a password for plaintext authentication of a Level-2 routing domain.

  domain-password [**0** | **7**] *password-string* [**send-only**]

  The Level-2 area authentication password function is disabled by default.

  All IS-IS devices in Level-2 domain must be configured with the same authentication password. This command does not take effect if the **authentication mode** command has been run to configure authentication before.

- Specify the IS-IS routing domain authentication mode.

  authentication mode { **md5** | **text** } [**level-1** | **level-2**]

  The authentication function is disabled by default.

- Specify the key chain for IS-IS authentication.

  authentication key-chain *name-of-chain* [**level-1** | **level-2**]

  No authentication key chain is configured by default.

Authentication is not performed if no key chain is configured using the **key chain** command. In addition to the key chain command, you also need to run the **authentication mode** command to make IS-IS key chain authentication take effect.

- (Optional) Apply IS-IS authentication only to send packets.

  authentication send-only [**level-1** | **level-2**]

  Packets sent and received are authenticated by default.

1.15 Configuring IS-IS GR

1.15.1 Overview

As long as the network conditions remain unchanged, GR enables IS-IS to be restarted and restored to the pre-restart state without impact on data forwarding. This improves system reliability.

Two roles exist during the GR process: Restarter and Helper. Accordingly, the IS-IS GR function is divided into IS-IS GR Restart and IS-IS GR Help capabilities. A device with the GR Restart capability can send a GR request and execute GR. A device with the GR Help capability can receive a GR request and help its neighbor with GR implementation. The GR process starts when the Restarter sends a GR request. After receiving the GR request, the neighboring device enters Help mode to help the Restarter reestablish its LSDB while maintaining the neighbor relationship with the Restarter. The main GR working mechanism is as follows:

1.15.2 Restrictions and Guidelines

Specification

All products support the IS-IS GR Helper capability.

1.15.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Enable the IS-IS GR Restart capability.

graceful-restart

The IS-IS GR Restart capability is enabled by default.

(5) (Optional) Configure the maximum GR interval of a device.

graceful-restart grace-period *max-interval*

The maximum GR interval is **300** seconds by default.

(6) Enable the IS-IS GR Help capability.

graceful-restart helper disable

The IS-IS GR Helper function is enabled by default.

This command enables IS-IS to ignore the GR request sent by the device to be restarted.

1.16 Configuring IS-IS NSR

1.16.1 Overview

IS-IS nonstop routing (IS-IS NSR) helps improve system reliability. During the active/standby switchover of devices in distributed or Virtual Switch Unit (VSU) mode, user data traffic keeps being forwarded without interruption. Information that can be backed up includes command configuration, neighbor backup, and LSP DB.

NSR backs up relevant IS-IS information from the master Supervisor Engine to the slave Supervisor Engine of the distributed device, or from the master device to the salve device in VSU mode, so that the device can automatically recover the link state and regenerate a route upon active/standby switchover, without requiring help from neighbor devices during the recovery.

Compared with GR that needs the help of a neighbor, NSR does not need any help from neighbors.

1.16.2 Restrictions and Guidelines

- For the same IS-IS process, either NSP or GR is enabled, because they are exclusive.
- The switchover of distributed devices and VSU devices takes a period of time. If the IS-IS neighbor keepalive duration is less than the switchover duration, IS-IS neighbor relationship with the neighbor device is removed, and the services are interrupted during the switchover. Therefore, it is recommended that the IS-IS neighbor keepalive duration be set not less than the default value. When Fast Hello is enabled, the IS-IS neighbor keepalive duration is less than 1 second and the IS-IS neighbor relationship times out during the switchover, causing NSR failures. Therefore, it is recommended that Fast Hello be disabled when NSR is enabled.

1.16.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Enable the NSR function.

nsr

The NSR function is disabled by default.

1.17 Correlating IS-IS with BFD

1.17.1 Overview

Bidirectional Forwarding Detection (BFD) is used to test connectivity between devices. A link fault can be detected in as short as 150 ms. After IS-IS is correlated with BFD, IS-IS can sense the death of a neighbor in as short as 150 ms once a link is faulty. This accelerates route convergence and prevents traffic interruption.

Normally, BFD sends detection packets at millisecond intervals to detect the link state. When a link exception (such as a disconnected link) occurs, BFD can quickly detect it and instruct IS-IS to delete the neighbor relationship and the neighbor reachability information in LSPs. Then IS-IS recalculates and generates a new route to bypass the abnormal link, thus realizing fast convergence. With the introduction of new techniques such as the Multi-Service Transport Platform (MSTP), link congestion tends to occur during peak hours of data communication. BFD quickly detects the link exception and instructs IS-IS to delete the neighbor relationship and the neighbor reachability information in LSPs. Link switch is performed to bypass the congested link. A Hello packet for IS-IS neighbor detection is sent every 10s and its expiration time is 30s. The Hello packet can still be received normally when BFD detects an exception, and therefore an IS-IS neighbor relationship is reestablished quickly, causing the route to be restored to the congested link. Then BFD detects the abnormal link and link switch is performed again. This process is repeated, which makes the route be switched between the congested link and other links, causing repetitive flapping.

The anti-congestion option is used to avoid routing flapping in case of link congestion. After the option is configured, the IS-IS neighbor state is still kept alive when link congestion occurs, but the neighbor reachability information in LSPs is deleted. The route is switched to a normal link. When the congested link is restored, the neighbor reachability information in LSPs is recovered and the route is switched back, which avoids route flapping.

1.17.2 Restrictions and Guidelines

- You must configure BFD session parameters before you enable IS-IS correlation with BFD.
- When you run the **bfd up-dampening** command on an interface with IS-IS correlation with BFD, you must run the **bfd all-interfaces [anti-congestion]** command.
- When you run the **bfd all-interfaces [anti-congestion]** command, you must run the **bfd up-dampening** command on the interface. The two commands must be used together. If you run only one command, the anti-congestion feature may not take effect or other network exceptions may occur.
- IP routing may cause a neighbor's interface for BFD session setup to be inconsistent with the interface for outgoing BFD packets. If this happens, the BFD session cannot be set up.
- If a neighbor's interface for BFD session setup is inconsistent with the interface for outgoing BFD packets, the BFD session cannot be set up.

1.17.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Enable BFD correlation in IS-IS process mode.

bfd all-interfaces [**anti-congestion**]

The IS-IS correlation with BFD function is disabled on all interfaces by default.

(5) Return to the global configuration mode.

exit

(6) Enter the interface configuration mode.

interface *interface-type interface-number*

(7) Enable IS-IS correlation with BFD on an interface.

isis bfd [**disable** | **anti-congestion**]

The IS-IS correlation with BFD function is enabled on an interface by default if the **bfd all-interfaces** command is run. The IS-IS correlation with BFD function is not enabled on an interface if the **bfd all-interfaces** command is not run. The anti-congestion option is disabled by default.

1.18 Configuring the IS-IS Overload Bit

1.18.1 Overview

An IS-IS node is forced to configure the overload bit in a non-virtual LSP to instruct its IS-IS neighbors to avoid using the local node as a forwarding device.

1.18.2 Restrictions and Guidelines

- If the **on-startup** keyword is selected, the IS-IS node automatically enters overload state after restart. If the **on-startup** keyword is not selected, the IS-IS node enters overload state immediately after restart.
- The overload bit is used in the following three situations:
  - Device overload

    The local IS-IS node has overload issues, such as insufficient memory or full CPU load; as a result, its routing table has incomplete routes or does not have resource forwarding data. You can configure the overload bit in an LSP to instruct the neighbor to avoid using the local node as a forwarding device.

    To configure the overload bit, run the **set-overload-bit** command without the **on-startup** keyword. The overload bit can be configured or removed manually. When the local IS-IS node is restored, manually remove the command configuration; otherwise, the node is always in overload state.
  - Instantaneous black hole

    In the scenario described by RFC 3277, the IS-IS convergence speed is faster than the BGP speed; as a result, after an IS-IS node is restarted, a route may be instantaneously unreachable, which is called an instantaneous black hole. You can set the overload bit in an LSP to instruct the neighbor to avoid using the local node as a forwarding device until the specified time has elapsed.

    To set the overload bit, run the **set-overload-bit** command with the **on-startup** keyword. The overload bit can be configured or removed automatically by the IS-IS node based on the configuration. After the **on-startup** keyword is selected, the IS-IS node automatically enters instantaneous black hole state after restart. When a neighbor relationship is established, the IS-IS node sends an LSP with the overload bit to notify the neighbor that the local node enters instantaneous black hole (or overload) state and instruct

the neighbor to avoid using the local node as a forwarding device. After the specified time has elapsed, the IS-IS node immediately sends an LSP with the overload bit canceled to notify the neighbor that the local node has exited instantaneous black hole (or overload) state and can work as a forwarding device.

- Disabling real data forwarding on the local IS-IS node

  If you only need to connect the local IS-IS node to a production network for testing or to meet other functional requirements, but does not require the node to forward real data in the network, you can set the overload bit in an LSP to instruct the neighbor to avoid using the local node as a forwarding device.

  To set the overload bit, run the **set-overload-bit** command without the **on-startup** keyword. The overload bit can be configured or removed manually. You can set the **suppress** keyword based on requirements to limit the routing information carried in an LSP in case of overload. For example, internal and external routes can be suppressed, and only the local direct route is advertised. For example, the advertised direct route and the metric value to reach a neighbor are set to the maximum values.

1.18.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Configure the IS-IS overload bit.

set-overload-bit [**on-startup** { *overload-time* | **wait-for-bgp** [*bgp-convergence-time*] }] [**suppress** { **interlevel** | **external** | **max-metric** } *] [**level-1** | **level-2**]

A neighbor considers the local IS-IS node as a forwarding device to forward data by default.

1.19 Configuring IS-IS VRF

1.19.1 Overview

VPN routing and forwarding (VRF) is mainly used for local routing and packet. It avoids route conflict caused by use of the same prefix by multiple VPNs.

1.19.2 Restrictions and Guidelines

- The IS-IS instances bound with the same VRF table must be configured with different system IDs. The IS-IS instances bound with different VRF tables can be configured with the same system ID.
- One IS-IS instance can be bound with only one VRF table, but one VRF table can be bound to multiple IS-IS instances.
- When the VRF table bound to an IS-IS instance is changed, all IS-IS interfaces associated with the instance will be deleted. That is, the **ip router isis [tag] interface** configuration and the redistribution configuration in routing process configuration mode will be deleted.

1.19.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Configure IS-IS VRF.

vrf *vrf-name*

VRF binding of an IS-IS instance is disabled by default.

1.20 Configuring IS-IS MTR

1.20.1 Overview

The IS-IS MTR technique helps users deploy IPv6 unicast networks without the constraint on consistency between IPv4 and IPv6 unicast topology information.

1.20.2 Restrictions and Guidelines

- Metric-style must be set to **Wide** or **Transition** before you enable this function.
- The MTR feature will be disabled if Metric-style is set to **Narrow** or only one Level is configured to support Wide or Transition mode.

1.20.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS IPv6 address family configuration mode.

address-family ipv6 unicast

(4) Configure IS-IS MTR.

multi-topology [*transition*]

IS-IS is not configured with MTR by default. That is, IS-IS does not support IPv6 unicast topologies. Configure IS-IS SNMP.

1.21 Configuring IS-IS SNMP

1.21.1 Overview

Use the network management software to manage OSPF parameters and monitor the OSPF running status.

1.21.2 Restrictions and Guidelines

- The latest standards stipulate that the MIB operation can be performed on a single instance. By default, the MIB operation is performed on the first displayed IS-IS instance. Because multiple IS-IS instances can be configured, the administrator can use this command to specify the instances on which the MIB operation will be performed.

1.21.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IS-IS trap globally.

snmp-server enable traps [*isis*]

The SNMP agent is forbidden to send Trap messages to the NMS by default.

This command must be used with the **snmp-server host** command in global configuration mode so that trap messages can be sent.

(4) Configure an SNMP host globally.

snmp-server host { *ipv4-addrress* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**traps**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]

No SNMP host address is configured by default.

(5) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(6) Bind the instances on which the IS-IS MIB operation will be performed.

enable mib-binding

By default, the SNMP operation is performed on the first displayed IS-IS instance.

(7) Allow sending trap messages.

enable traps { **all** | *traps set* }

The IS-IS trap message sending function is disabled by default.

1.22 Enabling Super VLAN for IS-IS

1.22.1 Overview

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when IS-IS multicast packets are sent over a super VLAN containing multiple sub VLANs, the IS-IS multicast packets are replicated multiple times, which exceeds the processing capability of the device. As a result, a large number of packets are discarded, causing protocol flapping. In most scenarios, the IS-IS function does not need to be enabled on a super VLAN, and it is disabled by default. In some application scenarios, the IS-IS function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, you can decide to send multicast packets to a certain sub VLAN or to all sub VLANs as actually needed using this command. You must be cautious when configuring packet transmission to all sub VLANs, as

the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flapping.

1.22.2 Restrictions and Guidelines

- The IS-IS basic functions must be configured.
- The specified sub VLAN must be connected to neighbors.

1.22.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure IS-IS to run on a super VLAN.

isis subvlan [**all |** *vlan-id*]

The IS-IS function takes effect in super VLAN only and is disabled by default.

1.23 Configuring IS-IS Two-way Maintenance

1.23.1 Overview

In a large-scale network, a large number of packets are sent and received, which occupies lots of CPU and memory resources, causing some IS-IS packets to be delayed or discarded. If the time required for processing hello packets exceeds the neighbor relationship maintenance time, the corresponding neighbor relationship times out and is removed. If the two-way maintenance function is enabled, in addition to the hello packets, the LSP, CSNP, and PSNP packets from a neighbor can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist in the network. This prevents termination of the adjacency caused by delayed or discarded hello packets.

1.23.2 Restrictions and Guidelines

- The IS-IS basic functions must be configured.
- The neighbor relationship is successfully established.

1.23.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Enable the IS-IS two-way maintenance function.

two-way-maintain

The two-way maintenance function is enabled by default.

1.24 Configuring Extended Feature of IS-IS

1.24.1 Overview

IS-IS provides rich extended features that can be configured based on actual needs.

1.24.2 Configuration Tasks

The IS-IS extended feature configuration tasks are as follows and optional. Select tasks for configuration according to the actual condition.

- Configuring the Maximum Metric of a Neighbor
- Configuring the Maximum Number of Area Addresses
- Configuring SPF Calculation Interval
- Canceling Three-Way Handshake of a P2P Network
- Enabling TLV to Be Padded Based on Supported Protocol
- Configuring the Reachable Time of a Suppressed Neighbor
- Enabling Adjacency Event Output

1.24.3 Configuring the Maximum Metric of a Neighbor

1. Overview

In the Overlay scene where IS-IS is applied to Underlay, the Overlay tunnel may rely on Underlay routing. After the IS-IS neighbor is up, the Underlay route is reachable but the Overlay tunnel may not be created, which may lead to traffic interruption. This function can prevent traffic interruption.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Configure the maximum metric for the directly-connected route after the first neighbor is up.

max-metric on-neighbor-up *delay-time*

The metric of the directly-connected route is not set to the maximum value by default.

1.24.4 Configuring the Maximum Number of Area Addresses

1. Overview

Generally, an IS-IS process is configured with a NET address. During area reallocation, an IS-IS process can be configured with multiple NET addresses to ensure routing correctness. The system ID of multiple NET addresses must be the same. For Level-1 IS-IS routers, neighbor relationship can be created between the routers only when the maximum numbers of area addresses are the same.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Configure the maximum number of area addresses.

max-area-addresses *max-area-number*

The maximum number of area addresses is **3** by default.

1.24.5 Configuring SPF Calculation Interval

1. Overview

Increasing the maximum interval for performing SPF calculations can avoid frequent SPF calculations and waste of CPU resources. However, a larger interval also leads to slower responses to route changes.

2. Restrictions and Guidelines

- The first wait time for performing the SPF calculation is *initial-interval*. If the network is unstable, the SPF calculation trigger interval is smaller than *maximum-interval* and the second wait time for performing the SPF calculation is changed to *hold-interval*. A corresponding penalty is added to this interval: The next interval for the SPF calculation doubles the previous interval for the same SPF calculation, until the SPF calculation interval reaches the *maximum interval*. Subsequent SPF calculations are performed at the *maximum interval*. When the network becomes stable, the interval for performing the SPF calculation becomes greater than the *maximum interval*, and the wait time for performing the SPF calculation is restored to the *initial interval*.
- The value of the configured *initial-interval* cannot be greater than that of *maximum-interval*. Otherwise, the value of *initial-interval* is changed to that of *maximum-interval*.
- The value of the configured *hold-interval* cannot be greater than that of *maximum-interval*. Otherwise, the value of *hold-interval* is changed to that of *maximum-interval*.
- The value of the configured *initial-interval* cannot be greater than that of *hold-interval*. Otherwise, the value of *initial-interval* is changed to that of *hold-interval*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Configure the SPF calculation interval.

spf-interval [**level-1** | **level-2**] *maximum-interval* [*initial-interval hold-interval*]

By default, the maximum calculation interval of two SPF calculations is **10** seconds, the delay of the first SPF calculation is **50** ms, and the maximum interval for the first and second SPF calculations is **200** ms. Exponential backoff algorithm uses Level-1/Level-2. That is, it takes effect for Level-1 and Level-2 concurrently.

1.24.6 Canceling Three-Way Handshake of a P2P Network

1. Overview

Neighbor establishment in a P2P network requires three-way handshake. The neighbor relationship can be established only after the three-way handshake succeeds. If you want to accelerate neighbor establishment or there is device that does not support three-way handshake, you can run this command to cancel three-way handshake.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Cancel three-way handshake of a P2P network.

isis three-way-handshake disable

Three-way handshake is performed by default.

1.24.7 Enabling TLV to Be Padded Based on Supported Protocol

1. Overview

When network devices supporting IPv4 IS-IS, IPv6 IS-IS, and IPv4 IS-IS and IPv6 are configured to establish a neighbor relationship, the calculated routes may be unreachable, resulting in routing black holes. To prevent routing black holes, the TLV (#129) field of device IS-IS protocol is padded based on protocols supported by an instance, that is, IS-IS instances that establish a neighbor relationship need to support the same protocol.

2. Restrictions and Guidelines

The TLV (#129) field of the IS-IS protocol supported by devices of some vendors is padded based on protocols supported by an interface. In single topology mode, a Ruijie device connects to a device of another vendor, a loopback interface is configured on both devices, both IS-IS IPv4 IS-IS and IPv6 IS-IS are enabled, and only a single protocol stack (IPv4 IS-IS or IPv6 IS-IS) is configured on the interconnected interfaces of the two devices. The device of the other vendor sends TLV#129 (supporting only a single protocol stack) based on interfaces whereas Ruijie device sends TLV#129 (supporting dual protocol stacks) based on instances. As a result, the displayed neighbor status on the device of the other vendor is "Init". Ruijie devices failed to establish a neighbor relationship with the device of the other vendor. For this, the **interfaces-protocol-compatible** command can be configured to enable Ruijie devices to establish a neighbor relationship with devices of other vendors.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Configure the TLV field of the IS-IS protocol to be padded based on protocols supported by an interface.

interfaces-protocol-compatible

The TLV field of the IS-IS protocol is padded based on protocols supported by an interface by default.

1.24.8 Configuring the Reachable Time of a Suppressed Neighbor

1. Overview

After the interface neighbor is up, this command prevents the neighbor reachability information from being added to LSP so as to delay the routing calculation. When the timer expires, the neighbor reachability information is added to LSP to start the routing calculation. This function prevents the route calculation from using the old LSP, which may lead to route flapping.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the IS-IS routing process configuration mode.

router isis [*tag*]

(4) Suppress route calculation after the IS-IS neighbor is up.

isis suppress on-neighbor-up *delay-time*

The route calculation suppression function is disabled by default.

1.24.9 Enabling Adjacency Event Output

1. Overview

You can run a debug command to record neighbor state changes of IS-IS, but the command consumes many system resources. You can enable adjacency event output to avoid this issue.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable neighbor relationship event output.

log-adjacency-changes

The function of recording neighbor state changes of IS-IS is enabled by default without the debug command.

1.25 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** command to clear information.

Caution

Running the **clear** command during operation of the device may lose vital information and interrupt services.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2 Monitoring

Command	Purpose
clear clns neighbors	Clears all IS-IS neighbor relationship tables.
clear isis *	Clears all IS-IS data structures.
clear isis [*tag*] **counter**	Clears different statistical information of IS-IS.

Command	Purpose
show clns [*tag*] **is-neighbors** [*interface-type interface-number*] [**detail**]	Displays all IS-IS neighbors and provides device adjacency relationships.
show clns [*tag*] **neighbors** [*interface-type interface-number*] [**detail**]	Displays all IS neighbors and provides device information and adjacency relationship information about terminals.
show isis [*tag*] **counter**	Displays different statistical information of IS-IS.
show isis [*tag*] **database** [*FLAGS*] [*LEVEL*] [*LSPID*]	Displays LSP DB information.
show isis [*tag*] **frr** *ipv4-net-address/mask*	Displays the IS-IS IP FRR routing information.
show isis [*tag*] **graceful-restart**	Displays the state information related to IS-IS GR.
show isis [*tag*] **hostname**	Displays the relationship between the device name and system ID.
show isis [*tag*] **interface** [*interface-type interface-number*] [*counter*]	Displays the details of an IS-IS interface.
show isis [*tag*] **mesh-groups**	Displays the mesh group configuration of different interfaces.
show isis [*tag*] **neighbors** [**detail**]	Displays IS-IS neighbor information.
show isis [*tag*] **nsr**	Displays IS-IS NSR information.
show isis [*tag*] **virtual-neighbors**	Displays the neighbor information of virtual systems in IS-IS.
show isis [*tag*] **protocol**	Displays the protocol information of IS-IS.
show isis [*tag*] **topology** [**frr** { **self-originate** | *WORD* | **all** }] [**l1** | **l2** | **level-1** | **level-2**]	Displays the topology of IS-IS device connection.
show isis [*tag*] **ipv6 topology** [**l1** | **l2** | **level-1** | **level-2**]	Displays IS-IS IPv6 unicast topology information of IS-IS.
debug isis { **all** | **auth | events** | **frr** | **gr** | **ifsm** | **lsp** | **mtr** | **nfsm** | **nsm** | **nsr** | **pdu** | **distribute**| **mom** | **spf** | **warn** }	Enables IS-IS debugging.

1.26 Configuration Examples

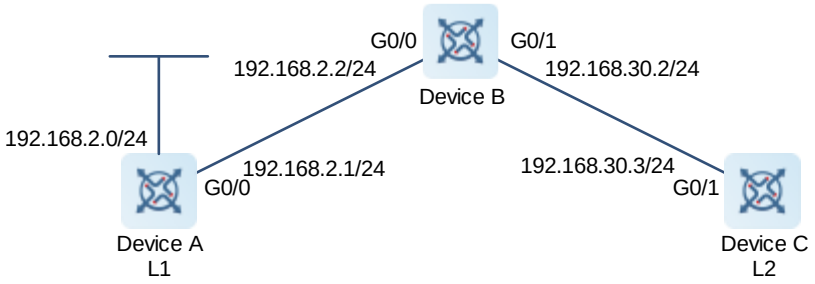
1.26.1 Performing Basic Authentication Configuration of IS-IS

1. Requirements

Devices A, B, and C are connected through the Ethernet and run IS-IS. Device A is a Level-1 device, Device B is a Level-1/Level-2 device, and Device C is a Level-2 device. The following configuration requirements exist: Plaintext authentication is applied to the Hello packets between Device A and Device B, as well as Level-1 LSPs and SNPs. MD5 authentication is applied to the Hello packets between Router B and Router C, as well as Level-2 LSPs and SNPs.

2. Topology

Figure 1-10 Topology of Basic Authentication Configuration of IS-IS



3. Notes

- Configure a key string.
- Configure IS-IS area authentication and interface authentication.

4. Procedure

(1) Configure IP addresses for interfaces.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitethernet 0/0
Device A(config-if-GigabitEthernet 0/0)# ip address 192.168.20.1 255.255.255.0
Device A(config-if)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface gigabitethernet 0/0
Device B(config-if-GigabitEthernet 0/0)# ip address 192.168.20.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/0)# exit
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.30.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip address 192.168.30.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/1)# exit
```

(2) Perform basic configuration of IS-IS.

Configure Device A.

```
Device A(config)# router isis
Device A(config-router)# net 49.0001.0000.0000.0001.00
Device A(config-router)# is-type level-1
Device A(config-router)# exit
Device A(config)# interface gigabitethernet 0/0
Device A(config-if-GigabitEthernet 0/0)# ip router isis
```

Configure Device B.

```
Device B(config)# router isis
Device B(config-router)# net 49.0001.0000.0000.0002.00
Device B(config-router)# exit
Device B(config)# interface gigabitethernet 0/0
Device B(config-if-GigabitEthernet 0/0# ip router isis
Device B(config-if-GigabitEthernet 0/0)# exit
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip router isis
Device B(config-if-GigabitEthernet 0/1)# exit
```

Configure Device C.

```
Device C(config)# router isis
Device C(config-router)# net 49.0002.0000.0000.0003.00
Device C(config-router)# is-type level-2
Device C(config-router)# exit
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip router isis
Device C(config-if-GigabitEthernet 0/1)# exit
```

(3) Enable IS-IS authentication.

Set the area authentication password of Device A to **aa**, and set the interface authentication password of GigabitEthernet 0/0 to **cc**.

```
Device A(config)# router isis
Device A(config-router)# area-password aa
Device A(config-router)# exit
Device A(config)# interface gigabitethernet 0/0
Device A(config-if-GigabitEthernet 0/0)# isis password cc
```

Configure Device B with Level-1 area plaintext authentication and set the key string to **kc1**; configure Level-2 area plaintext authentication and set the key string to kc**2**. Configure Device A with interface

plaintext authentication and set the key string to **kc3**. Configure Device C with interface MD5 authentication and set the key string to **kc3**.

```
Device B(config)# key chain kc1
Device B(config-keychain)# key 1
Device B(config-keychain-key)# key-string aa
Device B(config-keychain-key)# exit
Device B(config-keychain)# exit
Device B(config)# key chain kc2
Device B(config-keychain)# key 1
Device B(config-keychain-key)# key-string bb
Device B(config-keychain-key)# exit
Device B(config-keychain)# exit
Device B(config)# key chain kc3
Device B(config-keychain)# key 1
Device B(config-keychain-key)# key-string cc
Device B(config-keychain-key)# exit
Device B(config-keychain)# exit
Device B(config)# router isis
Device B(config-router)# authentication mode text level-1
Device B(config-router)# authentication key-chain kc1 level-1
Device B(config-router)# authentication mode md5 level-2
Device B(config-router)# authentication key-chain kc2 level-2
Device B(config-router)# exit
Device B(config)# interface gigabitethernet 0/0
Device B(config-if-GigabitEthernet 0/0)# isis authentication mode text
Device B(config-if-GigabitEthernet 0/0)# isis authentication key-chain kc3
Device B(config-if-GigabitEthernet 0/0)# exit
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# isis authentication mode md5
Device B(config-if-GigabitEthernet 0/1)# isis authentication key-chain kc3
```

Configure Device C with Level-2 area MD5 authentication and set the key string to **kc2**. Configure Device B with interface MD5 authentication and set the key string to **kc3**.

```
Device C(config)# key chain kc2
Device C(config-keychain)# key 1
Device C(config-keychain-key)# key-string bb
Device C(config-keychain-key)# exit
Device C(config-keychain)# exit
Device C(config)# key chain kc3
Device C(config-keychain)# key 1
Device C(config-keychain-key)# key-string cc
Device C(config-keychain-key)# exit
Device C(config-keychain)# exit
Device C(config)# router isis
Device C(config-router)# authentication mode md5 level-2
Device C(config-router)# authentication key-chain kc2
```

```
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# isis authentication mode md5
Device C(config-if-GigabitEthernet 0/1)# isis authentication key-chain kc3
```

5. Verification

Check the neighbor information of Device A.

```
Device A# show isis neighbors
Area (null):
System Id      Type  IP Address       State   Holdtime  Circuit          Interface
B            L1    192.168.20.2     Up     28       A.01            GigabitEthernet
0/0
```

Check the IS-IS database information of Device A.

```
Device A# show isis database detail
Area (null):
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime     ATT/P/OL
A.00-00           *  0x00000011   0xBE84       918             0/0/1
  Auth: TEXT(aa) Length: 3
  Area Address: 49.0001
  NLPID:       0xCC
  Hostname:    A
  IP Address:   192.168.20.1
  Metric:   1         IS A.01
  Metric:   1         IP 192.168.20.0 255.255.255.0
A.01-00           *  0x0000000A   0xF80A       918             0/0/0
  Auth: TEXT(aa) Length: 3
  Metric:   0         IS A.00
  Metric:   0         IS B.00
B.00-00              0x00000013   0xF62B       1129            1/0/0
  Auth: TEXT(aa) Length: 3
  Area Address: 49.0001
  NLPID:       0xCC
  Hostname:    B
  IP Address:   192.168.20.2
  Metric:   1         IS A.01
  Metric:   1         IP 192.168.20.0 255.255.255.0
  Metric:   1         IP 192.168.30.0 255.255.255.0
```

Check the neighbor information of Device B.

```
Device B# show isis neighbors
Area (null):
System Id      Type  IP Address       State   Holdtime  Circuit          Interface
C            L2    192.168.30.3     Up     21       B.02            GigabitEthernet
0/1
A            L1    192.168.20.1     Up     8        A.01            GigabitEthernet
0/0
```

Check the neighbor information of Device C.

```
Device C# show isis neighbors
Area (null):
System Id      Type  IP Address       State   Holdtime  Circuit          Interface
B            L2    192.168.30.2     Up      9        B.02            GigabitEthernet
0/0
```

6. Configuration Files

- Device A configuration file

```
!
router isis
 net 49.0001.0000.0000.0001.00
 is-type level-1
 area-password aa
!
interface gigabitethernet 0/0
 ip address 192.168.20.1 255.255.255.0
 ip router isis
 isis password cc
!
```

- Device B configuration file

```
!
key chain kc1
 key 1
  key-string aa
key chain kc2
 key 1
  key-string bb
key chain kc3
 key 1
  key-string cc
!
router isis
 net 49.0001.0000.0000.0002.00
 authentication mode text level-1
 authentication key-chain kc1 level-1
 authentication mode md5 level-2
 authentication key-chain kc2 level-2
!
interface gigabitethernet 0/0
 ip address 192.168.20.2 255.255.255.0
 ip router isis
 isis authentication mode text
 isis authentication key-chain kc3
!
```

```
interface gigabitethernet 0/1
 ip address 192.168.30.2 255.255.255.0
 ip router isis
 isis authentication mode md5
 isis authentication key-chain kc3
!
```

- Device C configuration file

```
!
key chain kc2
 key 1
  key-string bb
!
key chain kc3
 key 1
  key-string cc
!
router isis
 net 49.0002.0000.0000.0003.00
 is-type level-2
 authentication mode md5 level-2
 authentication key-chain kc2
!
interface gigabitethernet 0/1
 ip address 192.168.30.3 255.255.255.0
 ip router isis
 isis authentication mode md5
 isis authentication key-chain kc3
!
```

7. Common Errors

- Different authentication passwords are configured between neighbors.
- Different authentication modes are configured between neighbors.

1.26.2 Configuring IS-IS MTR

1. Requirements

The typical application scenario of MTR is to retain devices that only support IPv4 services in a network where IPv6 service extension will be performed.

As shown in Figure 1-11, Device B only supports the IPv4 protocol stack but does not support the MTR feature; therefore, it can only run IPv4 services. The network capacity needs to be scaled to support IPv6 services in order to meet service extension requirements. (Devices A, C, and D that support the MTR feature will be added.) Device B that supports only one protocol stack must be replaced to maintain the stability of the network running IPv4 and IPv6 dual protocol stacks; otherwise, IPv6 routing black holes may occur.

If you need to retain Device B, you can configure the MTR feature on the new devices. The MTR feature enables Device B to continue to run IPv4 services without interference on the IPv4 and IPv6 services on the

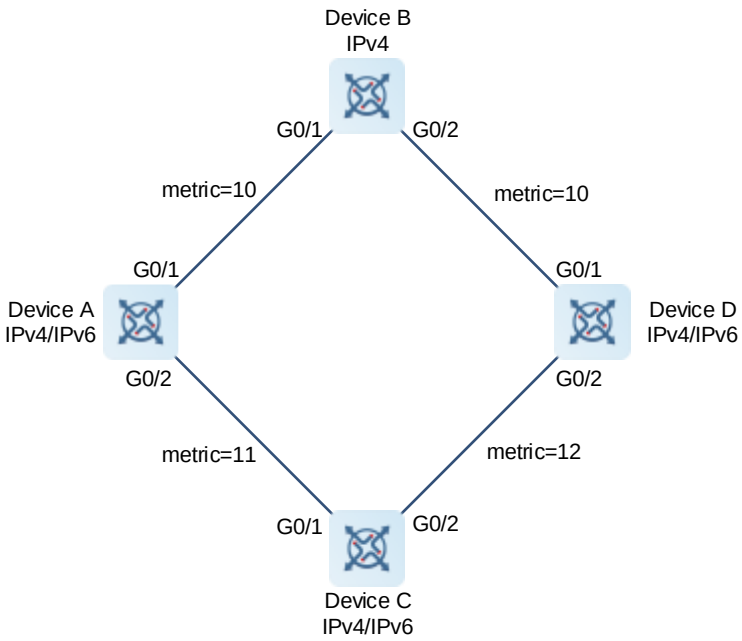
new devices. The MTR feature improves networking flexibility, indirectly prolongs the service life of old devices, and meets service extension requirements while maximizing the values of old devices.

The configuration requirements are as follows:

- Retain Device B, which only supports IPv4 services.
- Add devices that support IPv4 and IPv6 dual protocol stacks, and separate IPv4 route calculation and IPv6 route calculation.

2. Topology

Figure 1-11 Topology of IS-IS MTR Configuration



3. Notes

- Perform basic configuration of IS-IS.
- Enable the MTR function.

4. Procedure

- Configure Device A.

  Configure IS-IS, set the metric type to Wide, and enable the MTR function.

```
Device A> enable
Device A# configure terminal
Device A(config)# router isis
Device A(config-router)# net 49.0001. 0000.0000.0001.00
Device A(config-router)# is-type level-1
Device A(config-router)# metric-style wide
Device A(config-router)# address-family ipv6
Device A(config-router-af)# multi-topology
Device A(config-router-af)# exit
```

```
Device A(config-router)# exit
```

Configure an IP address for the interface and add the interface to IS-IS.

```
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ipv6 enable
Device A(config-if-GigabitEthernet 0/1)# ipv6 address 1002::1/112
Device A(config-if-GigabitEthernet 0/1)# ipv6 router isis
Device A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/1)# ip router isis
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface gigabitethernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ipv6 enable
Device A(config-if-GigabitEthernet 0/2)# ipv6 address 1003::1/112
Device A(config-if-GigabitEthernet 0/2)# ipv6 router isis
Device A(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/2)# ip router isis
Device A(config-if-GigabitEthernet 0/2)#isis wide-metric 11
```

- Configure Device B.

  Configure IS-IS, set the metric type to Wide, and enable the MTR function.

```
Device B> enable
Device B# configure terminal
Device B(config)# router isis
Device B(config-router)# net 49.0001. 0000.0000.0002.00
Device B(config-router)# is-type level-1
Device B(config-router)# metric-style wide
Device B(config-router)# address-family ipv6
Device B(config-router-af)# no adjacency-check
Device B(config-router-af)# exit
Device B(config-router)# exit
```

Configure an IP address for the interface and add the interface to IS-IS.

```
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# ip router isis
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface gigabitethernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ip address 192.168.3.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/2)# ip router isis
```

- Configure Device C.

  Configure IS-IS, set the metric type to Wide, and enable the MTR function.

```
Device C> enable
Device C# configure terminal
Device C(config)# router isis
Device C(config-router)# net 49.0001. 0000.0000.0003.00
Device C(config-router)# is-type level-1
Device C(config-router)# metric-style wide
```

```
Device C(config-router)# address-family ipv6
Device C(config-router-af)# multi-topology
Device C(config-router-af)# exit
Device C(config-router)# exit
```

Configure an IP address for the interface and add the interface to IS-IS.

```
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ipv6 enable
Device C(config-if-GigabitEthernet 0/1)# ipv6 address 3001::1/112
Device C(config-if-GigabitEthernet 0/1)# ipv6 router isis
Device C(config-if-GigabitEthernet 0/1)# ip address 192.168.2.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/1)# ip router isis
Device C(config-if-GigabitEthernet 0/1)#isis wide-metric 11
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface gigabitethernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ipv6 enable
Device C(config-if-GigabitEthernet 0/2)# ipv6 address 3004::1/112
Device C(config-if-GigabitEthernet 0/2)# ipv6 router isis
Device C(config-if-GigabitEthernet 0/2)# ip address 192.168.4.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/2)# ip router isis
Device C(config-if-GigabitEthernet 0/2)# isis wide-metric 12
```

- Configure Device D.

  Configure IS-IS, set the metric type to Wide, and enable the MTR function.

```
Device D> enable
Device D# configure terminal
Device D(config)# router isis
Device D(config-router)# net 49.0001.0000.0000.0004.00
Device D(config-router)# is-type level-1
Device D(config-router)# metric-style wide
Device D(config-router)# address-family ipv6
Device D(config-router-af)# multi-topology
Device D(config-router-af)# exit
Device D(config-router)# exit
```

Configure an IP address for the interface and add the interface to IS-IS.

```
Device D(config)# interface gigabitethernet 0/1
Device D(config-if-GigabitEthernet 0/1)# ipv6 enable
Device D(config-if-GigabitEthernet 0/1)# ipv6 address 4002::1/112
Device D(config-if-GigabitEthernet 0/1)# ipv6 router isis
Device D(config-if-GigabitEthernet 0/1)# ip address 192.168.3.4 255.255.255.0
Device D(config-if-GigabitEthernet 0/1)# ip router isis
Device D(config-if-GigabitEthernet 0/1)# exit
Device D(config)# interface gigabitethernet 0/2
Device D(config-if-GigabitEthernet 0/2)# ipv6 enable
Device D(config-if-GigabitEthernet 0/2)# ipv6 address 4003::1/112
Device D(config-if-GigabitEthernet 0/2)# ipv6 router isis
```

```
Device D(config-if-GigabitEthernet 0/2)# ip address 192.168.4.4 255.255.255.0
Device D(config-if-GigabitEthernet 0/2)# ip router isis
```

5. Verification

Run the **show** command on Device A to view IPv4 route information and check whether the next hop of the IPv4 route destined for Device D is Device B.

```
Device A# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
C   192.168.1.0/24 is directly connected, GigabitEthernet 0/1
C   192.168.1.1/32 is local host.
C   192.168.2.0/24 is directly connected, GigabitEthernet 0/2
C   192.168.2.1/32 is local host.
i L1 192.168.3.0/24 [115/20] via 192.168.1.2, 00:13:14, GigabitEthernet 0/1
i L1 192.168.4.0/24 [115/23] via 192.168.2.3, 00:02:40, GigabitEthernet 0/2
```

Run the **show** command on Device A to view IPv6 route information and check whether the next hop of the IPv6 route destined for Device D is Device C.

```
Device A# show ipv6 route
IPv6 routing table name is - Default - 16 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      O - OSPF intra area, OI - OSPF inter area,  OE1 - OSPF external type 1, OE2 -
OSPF external type 2
      ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
L     ::1/128 via Loopback, local host
C     1002::/112 via GigabitEthernet 0/1, directly connected
L     1002::1/128 via GigabitEthernet 0/1, local host
C     1003::/112 via GigabitEthernet 0/2, directly connected
L     1003::1/128 via GigabitEthernet 0/2, local host
I1    3001::/112 [115/21] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2
I1    3004::/112 [115/21] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2
I1    4002::/112 [115/31] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2
I1    4003::/112 [115/31] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2
L     FE80::/10 via ::1, Null0
C     FE80::/64 via GigabitEthernet 0/2, directly connected
L     FE80::1614:4BFF:FE12:ADFC/128 via GigabitEthernet 0/2, local host
C     FE80::/64 via GigabitEthernet 0/1, directly connected
L     FE80::1614:4BFF:FE12:ADFD/128 via GigabitEthernet 0/1, local host
C     FE80::/64 via Local 0, directly connected
L     FE80::1614:4BFF:FE12:ADFC/128 via Local 0, local host
```

6. Configuration Files

Device A configuration file

```
!
router isis
 net 49.0001. 0000.0000.0001.00
 is-type level-1
 metric-style wide
 address-family ipv6
  multi-topology
!
interface gigabitethernet 0/1
 ipv6 enable
 ipv6 address 1002::1/112
 ipv6 router isis
 ip address 192.168.1.1 255.255.255.0
 ip router isis
!
interface gigabitethernet 0/2
 ipv6 enable
 ipv6 address 1003::1/112
 ipv6 router isis
 ip address 192.168.2.1 255.255.255.0
 ip router isis
 isis wide-metric 11
!
```

Device B configuration file

```
!
router isis
 net 49.0001. 0000.0000.0002.00
 is-type level-1
 metric-style wide
 address-family ipv6
  no adjacency-check
!
 interface gigabitethernet 0/1
 ip address 192.168.1.2 255.255.255.0
 ip router isis
!
interface gigabitethernet 0/2
 ip address 192.168.3.2 255.255.255.0
 ip router isis
!
```

Device C configuration file

```
!
```

```
router isis
 net 49.0001. 0000.0000.0003.00
 is-type level-1
 metric-style wide
 address-family ipv6
  multi-topology
!
 interface gigabitethernet 0/1
 ipv6 enable
 ipv6 address 3001::1/112
 ipv6 router isis
 ip address 192.168.2.3 255.255.255.0
 ip router isis
 isis wide-metric 11
!
interface gigabitethernet 0/2
 ipv6 enable
 ipv6 address 3004::1/112
 ipv6 router isis
 ip address 192.168.4.3 255.255.255.0
 ip router isis
 isis wide-metric 12
!
```

Device D configuration file

```
!
router isis
 net 49.0001.0000.0000.0004.00
 is-type level-1
 metric-style wide
 address-family ipv6
  multi-topology
!
interface gigabitethernet 0/1
 ipv6 enable
 ipv6 address 4002::1/112
 ipv6 router isis
 ip address 192.168.3.4 255.255.255.0
 ip router isis
!
interface gigabitethernet 0/2
 ipv6 enable
 ipv6 address 4003::1/112
 ipv6 router isis
 ip address 192.168.4.4 255.255.255.0
 ip router isis
!
```

7. Common Errors

- The metric-style is not set to **Wide** or **Transition**.
- The protocol types used by two neighbors do not match; therefore, a neighbor relationship cannot be established.
- The IP addresses of the interfaces connected between neighbors are not in the same network segment.
- The **ip router isis** command is not executed on interfaces.
- No NET address is configured, or different NET addresses exist at Level-1.
- max-area-addresses is configured differently on both sides.
- metric-style is configured differently on both sides.
- The interface Levels on both sides are different. One side is Level-1, whereas the other side is Level-2.
- One side is configured with the P2P mode, whereas the other side is configured with the broadcast mode.
- One side is enabled with authentication, whereas the other side is not.

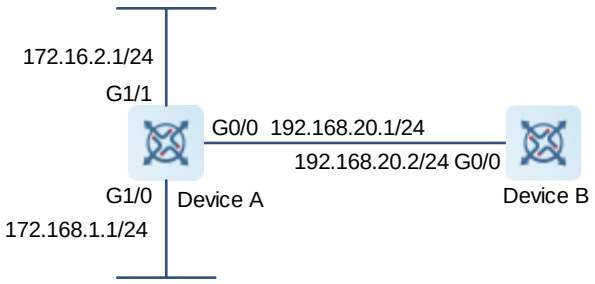
1.26.3 Configuring IS-IS Route Summarization

1. Requirements

Device A and Device B are connected through the Ethernet and run IS-IS. Device A is configured to advertise only the 172.16.0.0/22 route instead of the 172.16.1.0/24 and 172.16.2.0/24 routes.

2. Topology

Figure 1-12 Topology of IS-IS Route Summarization



3. Notes

- Configure IS-IS.
- Configure route summarization.

4. Procedure

(1) Configure IS-IS.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# router isis
Device A(config-router)# net 49.0001.0000.0000.0001.00
```

```
Device A(config-router)# exit
Device A(config)# interface gigabitethernet 0/0
Device A(config-if)# ip address 192.168.20.1 255.255.255.0
Device A(config-if)# ip router isis
Device A(config)# interface gigabitethernet 1/0
Device A(config-if)# ip address 172.16.1.1 255.255.255.0
Device A(config-if)# ip router isis
Device A(config)# interface gigabitethernet 1/1
Device A(config-if)# ip address 172.16.2.1 255.255.255.0
Device A(config-if)# ip router isis
Device A(config-if)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# router isis
Device B(config-router)# net 49.0001.0000.0000.0002.00
Device B(config-router)# exit
Device B(config)# interface gigabitethernet 0/0
Device B(config-if)# ip address 192.168.20.2 255.255.255.0
Device B(config-if)# ip router isis
```

(2) Configure route summarization.

Configure Device A.

```
Device A(config)# router isis
Device A(config-router)# summary-address 172.16.0.0/16 level-1-2
```

5. Verification

Run the **show ip route** command on Device B to check whether only one summary route exists.

```
Device B# show ip route
i L1   172.16.0.0/16 [115/20]  via 192.168.20.1, FastEthernet0/0
```

6. Configuration Files

- Device A configuration file

```
!
router isis
 net 49.0001.0000.0000.0001.00
 summary-address 172.16.0.0/16 level-1-2
!
interface gigabitethernet 0/0
 ip address 192.168.20.1 255.255.255.0
 ip router isis
!
interface gigabitethernet 1/0
 ip address 172.16.1.1 255.255.255.0
 ip router isis
```

```
!
interface gigabitethernet 1/1
 ip address 172.16.2.1 255.255.255.0
 ip router isis
!
```

- Device B configuration file

```
!
router isis
 net 49.0001.0000.0000.0002.00
!
interface gigabitethernet 0/0
 ip address 192.168.20.2 255.255.255.0
 ip router isis
!
```

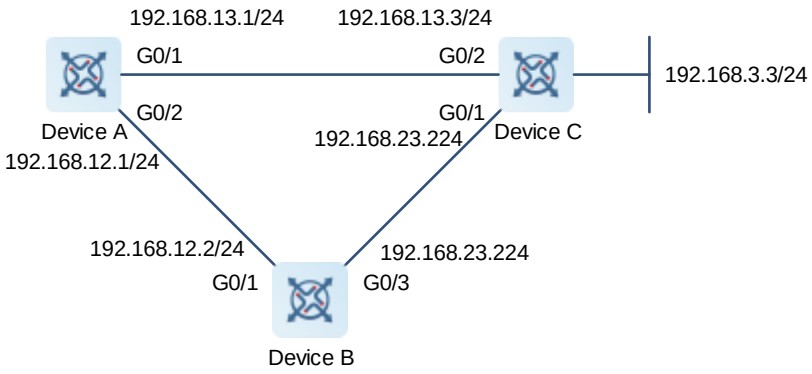
1.26.4 Correlating IS-IS with BFD

1. Requirements

Devices A, B, C, and D are interconnected through IS-IS routing protocol. The devices are Level-2 devices. When a link from Device A to Device C fails, services can be quickly switched to Device B.

2. Topology

Figure 1-13 Topology for IS-IS Correlation with BFD



3. Notes

- Configure interface IP addresses for all the devices.
- Configure the basic IS-IS functions on all devices.
- Enable the BFD function in the IS-IS routing process mode.

4. Procedure

(1) Configure interface IP addresses and perform basic configuration of IS-IS.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitethernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ip address 192.168.12.1/24
Device A(config-if-GigabitEthernet 0/2)# ip router isis
Device A(config-if-GigabitEthernet 0/2)# exit
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip address 192.168.13.1/24
Device A(config-if-GigabitEthernet 0/1)# ip router isis
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# router isis
Device A(config-router)# net 49.0001.0000.0000.0001.00
Device A(config-router)# is-type level-2-only
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface gigabitethernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.12.2/24
Device B(config-if-GigabitEthernet 0/1)# ip router isis
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface gigabitethernet 0/3
Device B(config-if-GigabitEthernet 0/3)# ip address 192.168.23.2/24
Device B(config-if-GigabitEthernet 0/3)# ip router isis
Device B(config-if-GigabitEthernet 0/3)# exit
Device B(config)# router isis
Device B(config-router)# net 49.0001.0000.0000.0002.00
Device B(config-router)# is-type level-2-only
```

Configure Device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# interface gigabitethernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ip address 192.168.13.3/24
Device C(config-if-GigabitEthernet 0/2)# ip router isis
Device C(config-if-GigabitEthernet 0/2)# exit
Device C(config)# interface gigabitethernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip address 192.168.23.3/24
Device C(config-if-GigabitEthernet 0/1)# ip router isis
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# router isis
Device C(config-router)# net 49.0001.0000.0000.0003.00
Device C(config-router)# is-type level-2-only
```

(2) Correlate IS-IS with BFD globally.

Configure Device A.

```
Device A(config-router)# bfd all-interfaces
```

Configure Device B.

```
Device B(config-router)# bfd all-interfaces
```

Configure Device C.

```
Device C(config-router)# bfd all-interfaces
```

5. Verification

- Normal network environment

  Check the routing table of Device A.

```
Device A# show ip route isis
I L2  192.168.23.0/24 [115/2] via 192.168.13.3, 00:19:07, GigabitEthernet 0/1
                      [115/2] via 192.168.12.2, 00:19:07, GigabitEthernet 0/2
I L2  192.168.33.0/24 [115/1] via 192.168.13.3, 00:17:40, GigabitEthernet 0/1
```

  Run **traceroute 192.168.3.3** on Device A.

```
Device A# traceroute 192.168.3.3
  < press Ctrl+C to break >
Tracing the route to 192.168.3.3

 1      192.168.3.3    <1 msec    5 msec    9 msec
```

- Link from Device A to Device C fails

  Check the routing table of Device A.

```
Device A# show ip route isis
I L2  192.168.23.0/24 [115/2] via 192.168.12.2, 00:00:08, GigabitEthernet 0/2
I L2  192.168.33.0/24 [115/2] via 192.168.12.2, 00:00:08, GigabitEthernet 0/2
```

  Run **traceroute 192.168.3.3** on Device A.

```
Device A# traceroute 192.168.3.3
  < press Ctrl+C to break >
Tracing the route to 192.168.3.3

 1      192.168.12.2     9 msec    8 msec   13 msec
 2      192.168.3.3      8 msec   10 msec    9 msec
```

6. Configuration Files

- Device A configuration file

```
!
interface gigabitethernet 0/2
 ip address 192.168.12.1/24
 ip router isis
!
interface gigabitethernet 0/1
 ip address 192.168.13.1/24
 ip router isis
!
router isis
```

```
 net 49.0001.0000.0000.0001.00
 is-type level-2-only
!
```

- Device B configuration file

```
!
interface gigabitethernet 0/1
 ip address 192.168.12.2/24
 ip router isis
!
interface gigabitethernet 0/3
 ip address 192.168.23.2/24
 ip router isis
!
router isis
 net 49.0001.0000.0000.0002.00
 is-type level-2-only
!
```

- Device C configuration file

```
!
interface gigabitethernet 0/2
 ip address 192.168.13.3/24
 ip router isis
!
interface gigabitethernet 0/1
 ip address 192.168.23.3/24
 ip router isis
!
router isis
 net 49.0001.0000.0000.0003.00
 is-type level-2-only
!
```

Contents

1 Configuring BGP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Concepts 1
1.1.3 Route Attributes 2
1.1.4 Route Exchange and Route Selection Policy of BGP 4
1.1.5 Neighbor Connection Establishment 6
1.1.6 Multi-path Load Balancing of BGP 7
1.1.7 Route Reflector 7
1.1.8 BGP Alliance 8
1.1.9 Route Aggregation 8
1.1.10 Route Dampening 8
1.1.11 BGP Reliability 9
1.1.12 BMP 11
1.1.13 Others 12
1.1.14 Protocols and Standards 12
1.2 Configuration Task Summary 13
1.3 Configuring BGP Basic Features 14
1.3.1 Configuration Tasks 14
1.3.2 Configuring a BGP Neighbor 14
1.3.3 Configuring a BGP IPv6 Address Family 16
1.3.4 Configuring a BGP Peer Group 17

1.3.5 Configuring the Dot Mode to Display 4-Byte AS Numbers 18

1.3.6 Configuring Routing Information Advertisement 18

1.3.7 Configuring Multi-Path Route Import Between VRF Instances 19

1.3.8 Shutting Down BGP Connections Gracefully 20

1.3.9 Configuring BGP Soft Reset 21

1.3.10 Configuring Route Update Mechanisms of BGP 22

1.3.11 Configuring BGP Capacity Protection 23

1.4 Configuring a large BGP Network 25

1.4.1 Configuration Tasks 25

1.4.2 Configuring a Route Reflector 25

1.4.3 Configuring an AS Alliance 26

1.4.4 Configuring Route Aggregation 27

1.4.5 Configuring Route Dampening 27

1.5 Configuring BGP Route Selection and Load Balancing 28

1.5.1 Configuration Tasks 28

1.5.2 Configuring Multi-path Load Balancing of BGP 28

1.5.3 Configuring BGP Routes to Be Recursive Only to Host Routes 29

1.5.4 Configuring Outbound Loop Detection for a BGP Neighbor 30

1.5.5 Configuring BGP ADD-PATH 31

1.5.6 Configuring BGP to Advertise Routes with the Lowest Priority upon Device Restart 32

1.5.7 Configuring the AS_PATH Attribute 32

1.6 Configuring BGP to Control Route Advertisement and Receiving 33

1.6.1 Configuration Tasks 33

1.6.2 Configuring Fast Withdrawal of Specified BGP Routes 33

1.6.3 Configuring Delayed Route Advertisement of BGP 34

1.7 Configuring the BGP Security Function 35

1.7.1 Overview 35

1.7.2 Configuring MD5 Authentication 35

1.7.3 Configuring the Generalized TTL Security Mechanism (GTSM) Security Check for BGP Neighbors 36

1.8 Configuring BGP Reliability 37

1.8.1 Configuration Tasks 37

1.8.2 Configuring BFD For BGP 37

1.8.3 Configuring BGP FRR 38

1.8.4 Configuring EBGP Multi-Path Bypass Protection 39

1.8.5 Configuring BGP GR 40

1.8.6 Configuring BGP NSR 40

1.8.7 Configuring BGP Session Retention 41

1.9 Enabling the Extended Functions of BGP 42

1.9.1 Configuration Tasks 42

1.9.2 Configuring BMP Monitoring 42

1.9.3 Configuring the Administrative Distance of BGP 44

1.10 Monitoring 45

1.11 Configuration Examples 47

1.11.1 Configuring BGP Basic Networking 47

1.11.2 Configuring BGP MD5 Authentication 55

1.11.3 Configuring a BGP Route Reflector 61

1.11.4 Configuring a BGP Alliance 65

1.11.5 Configuring IBGP Multi-Path Load Balancing 73

1.11.6 Configuring EBGP FRR 76

1.11.7 Configuring BGP to Rapidly Withdraw Specified Routes 81

1.11.8 Configuring the BGP Local AS 82

1.11.9 Configuring BGP GR 85

1.11.10 Configuring IPv6 Route Exchange Across ASs 88

1.11.11 Configuring Compatibility Between BGP Devices Supporting 4-Byte AS Numbers and Those Supporting 2-Byte AS Numbers 91

1.11.12 Configuring an IPv6 Local Link Address 93

1.11.13 Configuring BGP NSR 96

1.11.14 Configuring BGP Routes to Be Recursive Only to Host Routes 98

1.11.15 Configuring Outbound Loop Detection for a BGP Neighbor 99

1.11.16 Shutting Down BGP Connections Gracefully 102

1.11.17 Configuring BGP Multi-Path Bypass Protection 105

1.11.18 Configuring Multi-Path Route Import Between VRF Instances 109

1.11.19 Configuring BMP Monitoring 115

1.11.20 Configuring BGP ADD-PATH 116

1 Configuring BGP

1.1 Introduction

1.1.1 Overview

The Border Gateway Protocol (BGP) is a dynamic routing protocol that automatically exchanges loop-free routing information between autonomous systems (ASs).

A network is divided into multiple ASs to facilitate management. In the early Internet, the Exterior Gateway Protocol (EGP) was used to switch routing information between ASs. This protocol was first mentioned in RFC 187 and then listed into RFC 904 in 1984. EGP was a simple network reachability protocol and applied only to tree networks. Therefore, it could not meet the increasingly complicated network management requirements and finally was replaced by BGP. Unlike EGP, BGP can avoid loops and select better routes, and efficiently transfers routes and supports higher scalability.

The development of BGP has undergone different stages, and BGP-1 (RFC 1105), BGP-2 (RFC 1163), and BGP-3 (RFC 1267) were previously released. The prevailing version is BGP-4 (RFC 4271), which is widely applied between ASs as a standard routing protocol.

BGP has the following features:

- Interior Gateway Protocols (IGPs) such as Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) focus on discovery and route calculation. By contrast, BGP lays emphasis on the control of route spreading and is applicable to networks that carry massive routes.
- BGP uses Transmission Control Protocol (TCP) as the transmission protocol and the destination port is 179. BGP uses the reliable transmission mechanism of TCP to ensure transmission reliability.
- As a distance vector routing protocol, BGP transmits only the locally selected optimal routes to its neighbors.

Note

In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be Layer-3 (L3) switches, routers, or firewalls.

1.1.2 Concepts

1. BGP speaker

Devices that run BGP and send BGP packets are called BGP speakers.

2. BGP peer

BGP speakers with a BGP session established are BGP peers. Multiple peers constitute a peer group.

3. AS

Devices that manage and share the same routing policies in one organization are an AS. When BGP is enabled on a router, a local AS number must be specified for it. An AS number is a globally unique number allocated by IANA, consisting of two or four bytes.

A traditional AS number consists of 2 bytes, ranging from 1 to 65535. The new 4-byte AS numbers aims to resolve the resource exhaust problem, and their value range is from 1 to 4294967295.

4-byte AS numbers support two expression modes: decimal notation mode and dot mode. The decimal notation mode is the same as the traditional expression mode, that is, the 4 bytes of an AS number are expressed in decimal notation. The conversion relationship between the dot mode and decimal notation mode is as follows: 4-byte decimal AS number = x × 65536 + Y.

For example:

- For an AS number 65534 in decimal mode, it is 65,534 in dot mode. An AS number smaller than 65536 is the same in decimal mode and dot mode.
- For an AS number 65536 in decimal mode, it is 1.0 in dot mode.
- For an AS number 65538 in decimal mode, it is 1.2 in dot mode.

With introduction of 4-byte AS numbers, BGP connections may be established between BGP speakers supporting only 2-byte AS numbers and those supporting 4-byte AS numbers. To communicate with a device that supports 4-byte AS numbers, reserve the AS number 23456 for filling on the device that supports only 2-byte AS numbers.

4. Neighbor type and route type

BGP neighbors are classified into two types:

- Internal BGP (IBGP) neighborship: The neighborship between BGP speakers within an AS is called IBGP neighborship. Routes learned from IBGP neighbors are called IBGP routes. IBGP completes transition of routing information within the AS.
- External BGP (EBGP) neighborship: The neighborship between BGP speakers in different ASs is called EBGP neighborship. Routes learned from EBGP neighbors are called EBGP routes. EBGP is used to exchange routing information between different ASs.

1.1.3 Route Attributes

When a BGP speaker advertises a route to its neighbors, the BGP speaker also advertises the attributes carried by the route. Common BGP attributes are as follows:

1. Origin attribute

Specifies the origin of a BGP route, which is set to IGP, EGP, or INCOMPLETE.

- IGP: The value is 0, specifying the internal routing information of the originating AS.
- EGP: The value is 1, specifying the routing information obtained from EGP.
- INCOMPLETE: The value is 2, specifying the routing information learned through other means.

2. AS_PATH attribute

Lists the ASs passed by a route reversely. The last AS is placed at the beginning of the list.

The AS_PATH attribute is used for:

- When a router receives routing information with the local AS number in the AS_PATH, the router considers that this route has loop and discards the packet.
- Routing information distribution is controlled by using the AS_PATH-based filtering rules. These filtering rules use regular expressions to parse AS paths.

- According to RFC 1771, BGP does not consider the AS path length when selecting an optimal path. Generally, a shorter AS path means a higher path priority; therefore, devices consider the AS path length when selecting the optimal path. Based on the actual condition, you can determine whether to consider the AS path length when selecting the optimal path.

3. NEXT_HOP attribute

Specifies the IP address of the next hop to be reached by a BGP route.

The change in the NEXT_HOP attribute complies with the following rules:

- When the route forwarded to an IBGP peer is non-local, the device does not change the NEXT_HOP attribute.
- When the route forwarded to an IBGP peer is local, the local interface address that the device uses to establish a BGP neighbor relationship with the peer is the next hop address.
- When the route is forwarded to an EBGP peer, the local interface address that the device uses to establish a BGP neighbor relationship with the peer is the next hop address.

4. MULTI_EXIT_DISC attribute

Distinguishes multiple output or input points for reaching the same neighbor AS. A smaller value means a higher priority. The MULTI_EXIT_DISC attribute is short for MED.

BGP uses the MED value as the basis for comparing priorities of paths learned from EBGP peers. A smaller MED value means a higher path priority.

- The **MED** value is compared only for paths of peers from the same AS during the optimal path selection by default.
- The **MED** value is not compared for paths of peers from other member ASs in an AS alliance during the optimal path selection by default.
- If a path not configured with the MED attribute is received, the MED value of this path is **0** by default. Since a smaller MED value means a higher path priority, the MED value of this path has the highest priority.
- The **MED** value is not compared for paths from different ASs during the optimal path selection by default. Instead, the receiving sequence of the paths is compared.

5. LOCAL_PREF attribute

Distinguishes the priorities of IBGP routes in an AS. A larger value means a higher priority.

When sending routes received from EBGP peers to IBGP peers, a BGP speaker adds the LOCAL_PREF attribute. BGP uses the LOCAL_PREF value as the basis for comparing priorities of paths learned from IBGP peers. A larger LOCAL_PREF value means a higher path priority.

6. COMMUNITY attribute

The **COMMUNITY** attribute is another method of controlling the distribution of routing information.

A community is a set of destination addresses. The **COMMUNITY** attribute is intended to facilitate execution of a community-based routing policy so as to simplify the configuration of routing information distribution control on BGP speakers. By using the community attribute, you can control the receiving and distribution of routing information. A destination address can belong to multiple communities. An AS administrator can define the communities, to which a destination address belongs.

BGP pre-defines four common community attribute values:

- **Internet**: Indicates the Internet community. All paths belong to this community.
- **No-export**: Specifies that the path is not advertised to EBGP peers.
- **No-advertise**: Specifies that the path is not advertised to any BGP peer.
- **Local-as**: Indicates that a path is not advertised outside the local AS. When an alliance is configured, the path is not advertised to other ASs or member ASs.

By default, all destination addresses belong to the Internet community and are carried in the **COMMUNITY** attribute of paths.

BGP speakers can set, add, or modify the community attribute value when learning, advertising, or re-distributing routes. An aggregate path will contain the community attribute values of all aggregated paths.

7. AIGP metric attribute

The AIGP metric attribute can accumulate the IGP metrics of paths that a route passes through. Preferred route selection based on the AIGP attribute value can reflect the path cost more accurately. A smaller AIGP attribute value indicates a higher route priority. Routes carrying the AIGP attribute have a higher priority than those without the AIGP attribute.

If the next hop of a route carrying the AIGP attribute is changed to self or another value during route transmission, the IGP metric value of the route to the original next-hop address needs to be added to the AIGP attribute value.

1.1.4 Route Exchange and Route Selection Policy of BGP

1. Route exchange

BGP cannot automatically discover or learn accessible networks. The accessible network information of a local AS must be imported to BGP so that BGP can advertise this information to neighbors.

Two methods can be used to import network information of the local AS to BGP:

- Manual configuration: Import accessible network information within a specified range to BGP.
- Configuring route re-distribution: Configure route re-distribution to re-distribute accessible network information of IGP to BGP.

BGP offers a robust route management function. By configuring a route exchange policy for a BGP peer, you can actively control routes to be received by and to be advertised to this peer.

Send routing information of other ASs exchanged by BGP to the routing table of a device so that the device can forward packets of other ASs. Import routing information of other ASs exchanged by BGP to IGP so that IGP distributes the information to other IGP devices in the local AS and these devices can forward packets of other ASs.

Generally, BGP speakers serving as IBGP neighbors of each other are not directly connected physically. IGP devices in the link between the BGP speakers may fail to learn routing information same as that on the BGP speakers. When a BGP speaker at the border of an AS forwards packets received from other domains to the next-hop IBGP neighbor, the packets pass an IGP device in the middle. In this case, the packets may be lost due to no routing information on the IGP device. To synchronize BGP with IGP, you must ensure that all routers within an AS learn routing information to be sent to another AS before the routing information is advertised to this AS. BGP and IGP should be synchronized in most cases, except that:

- Routing information passing through this AS is not configured. For example, the AS is a stub AS.

- All routers within the AS run BGP. Full mesh is established among all BGP speakers (neighborship is established between each two BGP speakers).

2. BGP route update group

The BGP route update group function is a technology used to enhance the performance for advertising routes to neighbors.

The BGP route update group technology automatically classifies neighbors using the same policy into the same update group. When sending a route to a neighbor, the device encapsulates the update packet based on the update group, and sends the update packet to all neighbors in the update group. In this way, the update packet is encapsulated only once but sent multiple times, improving the performance of route advertisement to neighbors.

3. Route selection policy

BGP policies for selecting the optimal route are:

(1) Invalid routing entries (entries with the next hop unreachable and flapping entries) are not used for optimal route selection.

(2) If not, the route generated by the **network** command is preferred.

(3) Otherwise, a route with the maximum weight is preferred (the default weight value of a route originated locally is **32768**, and the weight value of a router advertised by a neighbor is **0**).

(4) If routes have the same weight, a route with a larger **LOCAL_PREF** value is preferred.

(5) If routes have the same local priority, a local BGP route from the local router is preferred.

(6) The types of local routes are compared, and the route priority is as follows: direct route > static route > aggregate route generated by BGP.

(7) If the local routes have the same type, the Accumulated Interior Gateway Protocol (AIGP) extended route is compared. A route that carries the AIGP attribute is prior to that without the AIGP attribute.

(8) If the AIGP attribute comparison is skipped, the link state (LS) extended attribute is compared:

a A route with the LS attribute is preferred.

b A route with a smaller IGP metric is preferred.

c A route of the wide type has a higher priority than that of the narrow type.

(9) Otherwise, a route with the shortest AS length is selected.

(10) Otherwise, a route with the lowest **ORIGIN Code** attribute value is selected.

(11) Otherwise, a route with the smallest **MED** value is selected.

(12) Otherwise, EBGP routes have a higher priority than IBGP routes and routes in an AS alliance, and the IBGP routes have the same priority as the routes in an AS alliance.

(13) Otherwise, a route with the smallest IGP metric value to the next hop is selected.

(14) Otherwise, an EBGP route that is received first is selected.

(15) Otherwise, a route advertised by a BGP speaker with a smaller router-ID is selected.

(16) Otherwise, a route with a smaller cluster length is selected.

(17) Otherwise, a route with a smaller neighbor address is selected.

1.1.5 Neighbor Connection Establishment

A BGP neighbor is manually configured by a user. Neighbor relationships can be established in two modes: IBGP and EBGP. Users can identify the connection mode between BGP speakers according to the AS carrying the BGP peer and the AS carrying the BGP speaker.

A BGP speaker proactively sends a TCP connection request to a specified BGP peer. After a TCP connection is established successfully, BGP speakers exchange BGP protocol packets to negotiate about connection parameters. The BGP neighbor relationship is successfully established after the negotiation succeeds.

1. Establishing a TCP connection

A BGP speaker initiates a TCP connection request to a neighbor. The destination IP address of the request is the peer IP address specified by the user and the port number is fixed to **179**.

The BGP speaker also listens on port 179 of the local TCP connection to receive connection requests from its peers.

2. Negotiating about protocol parameters

After a TCP connection is successfully established, BGP speakers exchange OPEN packets to negotiate about BGP connection parameters. Negotiated parameters include the following:

- **Version**: Indicates the BGP version number. At present, only version 4 is supported.
- **Neighbor AS number**: Determines whether the AS number of a neighbor is consistent with the AS number specified locally. If no, the connection request is denied.
- **Hold time**: Indicates the timeout duration for a BGP connection. The default value is **180** seconds.
- **Neighbor capability**: Negotiates about various extended capabilities supported by the neighbor, including the address family, dynamic route update and GR functions.

3. Maintaining the neighbor relationship

BGP speakers send the Keepalive message to each other periodically. If a new Keepalive packet is not received from a BGP neighbor after the hold time expires, the BGP speaker considers the neighbor unreachable, disconnects the TCP connection from the neighbor, and attempts to reconnect to it. The interval for a BGP speaker to send the Keepalive message is one third of the negotiated hold time and is **60** seconds by default.

The software allows you to manually configure various timers within BGP to meet the neighbor keepalive and route management requirements in different network environments.

- BGP neighbor keepalive timer

  BGP uses the keepalive timer to maintain a valid connection with a peer and the holdtime timer to judge whether the peer is valid. The default value of the keepalive timer is **60** seconds and the default value of the holdtime timer is **180** seconds. When BGP speakers establish a BGP connection, both parties negotiate about the holdtime and the smaller holdtime value is selected. The keepalive timer is set to one third of the negotiated holdtime value or the configured keepalive value, whichever is smaller.

- Neighbor reconnection timer

  To reduce the impact of frequent BGP reconnection to a failed neighbor on the network bandwidth, after a BGP speaker detects a neighbor connection failure, it attempts to reconnect to the neighbor after the Connect-Retry timer expires. The default value of the Connect-Retry timer is **15** seconds.

- Route advertisement timer

  To reduce the impact of route update packets on the network bandwidth, after a BGP speaker detects a network topology change, it does not advertise the route update to its neighbors immediately. Instead, the BGP speaker adopts a regular update mechanism to advertise all changed routing information to its neighbors.

1.1.6 Multi-path Load Balancing of BGP

Multi-path load balancing means that there are multiple paths to the same network and data packets are evenly forwarded by these paths. In this case, one route has multiple next hops in the routing table.

According to the types of equal-cost routes, multi-path load balancing of BGP is classified into the following types:

- EBGP load balancing: Implements load balancing for routes learned from EBGP neighbors.
- IBGP load balancing: Implements load balancing for routes learned from IBGP neighbors.

When there are multiple paths to the same network in the routing table of BGP, BGP calculates a route with the highest priority by default. If there are multiple optimal routes with the same priority, BGP still selects a unique route according to comparison rules, advertises the route to the forwarding plane, and controls the forwarding of data streams. After multi-path load balancing is enabled, in addition to calculating a unique optimal route, BGP lists paths with the same priority as the optimal route as equal-cost routes. Then, BGP advertises the optimal route and equal-cost routes to the forwarding plane to implement load balancing.

Equal-cost routes have the same basic attributes and priority. That is, according to the optimal path selection rules of BGP, paths have the same priorities before router-IDs are compared.

- AS_PATH loose comparison

  Equal-cost routes must have the same AS-PATH attribute by default. Under such strict conditions, load balancing cannot be implemented in certain environments. In this case, you are advised to enable the AS-PATH loose comparison mode. In AS-PATH loose comparison mode, when other conditions for equal-cost routes are met, equal-cost route conditions are met as long as the AS-PATH lengths of routes and the AS-PATH lengths of the member ASs are equal respectively.

- Router-ID multi-path comparison

  Equal-cost routes do not need to come from the same device (that is, the sources of the routes do not need to have the same router ID) by default. After the router-ID multi-path comparison is enabled, only routes with the same router-ID can be equal-cost routes.

- Non-equal-cost load balancing

  Load-balanced routes are equal-cost routes by default. After the non-equal-cost load balancing is enabled, you can configure routes to carry the Link-Bandwidth attribute so that non-equal-cost routes form.

1.1.7 Route Reflector

Route reflectors are a method of reducing IBGP peer connections in an AS.

According to the principle of BGP route advertisement, all BGP speakers in an AS must establish a full mesh of connections (every two BGP speakers need to establish a neighbor relationship). Too many BGP speakers in an AS will increase their resource cost, ramp up network administrators' configuration workload and complexity, and reduce the network expansion capacity.

You can configure a BGP speaker as a route reflector, which classifies IBGP peers in the AS into two types: clients and non-clients.

The rules for implementing a route reflector in an AS are as follows:

- Configure a route reflector and specify clients for the route reflector. The route reflector and its clients form a cluster. The route reflector will connect to its clients.
- The clients of a route reflector in a cluster cannot connect to BGP speakers outside the cluster.
- Within an AS, a full mesh of connections is established among IBGP peers of non-clients. The IBGP peers of non-clients include the following situations: Multiple route reflectors in a cluster; a route reflector in a cluster and BGP speakers (generally not supporting the route reflector function) not involved in the route reflector function out of the cluster; a route reflector in a cluster and route reflectors in other clusters.

The rules for processing a route received by a route reflector are as follows:

- A route update message received from an EBGP speaker will be sent to all clients and non-clients.
- A route update message received from a client will be sent to other clients and all non-clients.
- A route update message received from an IBGP non-client will be sent to all clients of the route reflector.

1.1.8 BGP Alliance

Alliances are another method of reducing IBGP peer connections in an AS.

You can divide an AS into multiple member ASs and configure a unified alliance ID (namely, alliance AS number) for these member ASs to form an alliance. Outside the alliance, the entire alliance is still considered as an AS and only the AS number of the alliance is visible. Inside the alliance, BGP speakers in a member AS still establish a full mesh of IBGP peer connections, BGP speakers in different member ASs establish EBGP connections. Though EBGP connections are established between BGP speakers in different member ASs, the NEXT_HOP, MED, LOCAL_PREF, and other path attributes keep unchanged during information exchange.

1.1.9 Route Aggregation

The great BGP routing table in a large network brings heavy load to BGP devices. BGP supports classless inter-domain routing (CIDR). Therefore, route aggregation entries can be created to reduce the size of the BGP routing table. BGP aggregation entries can be added to the BGP routing table only when valid paths are configured within the aggregation range. Routes can be manually aggregated on a device. Thus, this function can control whether to reserve AS path information within the aggregation address range, and whether to advertise only aggregated paths.

1.1.10 Route Dampening

If a route changes between the valid state and invalid state, route flapping occurs. Route flapping often causes the transmission of unstable routes in a network, and thereby causes network instability. BGP route dampening is a method of reducing route flapping. It reduces possible route flapping by monitoring routing information from EBGP peers.

Terms involved in BGP route dampening are as follows:

- **Route Flap**: A route changes between the valid sate and invalid state.
- **Penalty**: Once route flapping occurs, a BGP speaker, on which route dampening is enabled, adds a penalty value to this route. The penalty value accumulates until **Suppress Limit** is reached.
- **Suppress Limit**: When the penalty of a route is greater than this value, the route is suppressed.

- **Half-life-time**: It indicates the time required for the penalty to be halved.
- **Reuse Limit**: When the penalty value of a route is smaller than this value, route suppression is canceled.
- **Max-suppress-time**: It indicates the maximum time that a route can be suppressed.

A BGP speaker assigns a route a penalty (accumulated to the penalty value) each time the route flaps. When the penalty value reaches **Suppress Limit**, the route is suppressed. When the penalty value reaches **Half-life-time**, the penalty is halved. When the penalty value is reduced to **Reuse Limit**, the route is activated again. The maximum time that a route can be suppressed is the value of **Max-suppress-time**.

By default, the penalty value increases by 1000 when a route is reactivated and increases by 500 when a route is updated.

1.1.11 BGP Reliability

1. GR

Graceful restart (GR) is intended to ensure that data forwarding is not interrupted during the BGP restart. The GR function keeps the network topology stable, maintains the forwarding table, and ensures that key services are not interrupted during the switching of master and slave supervisor engines.

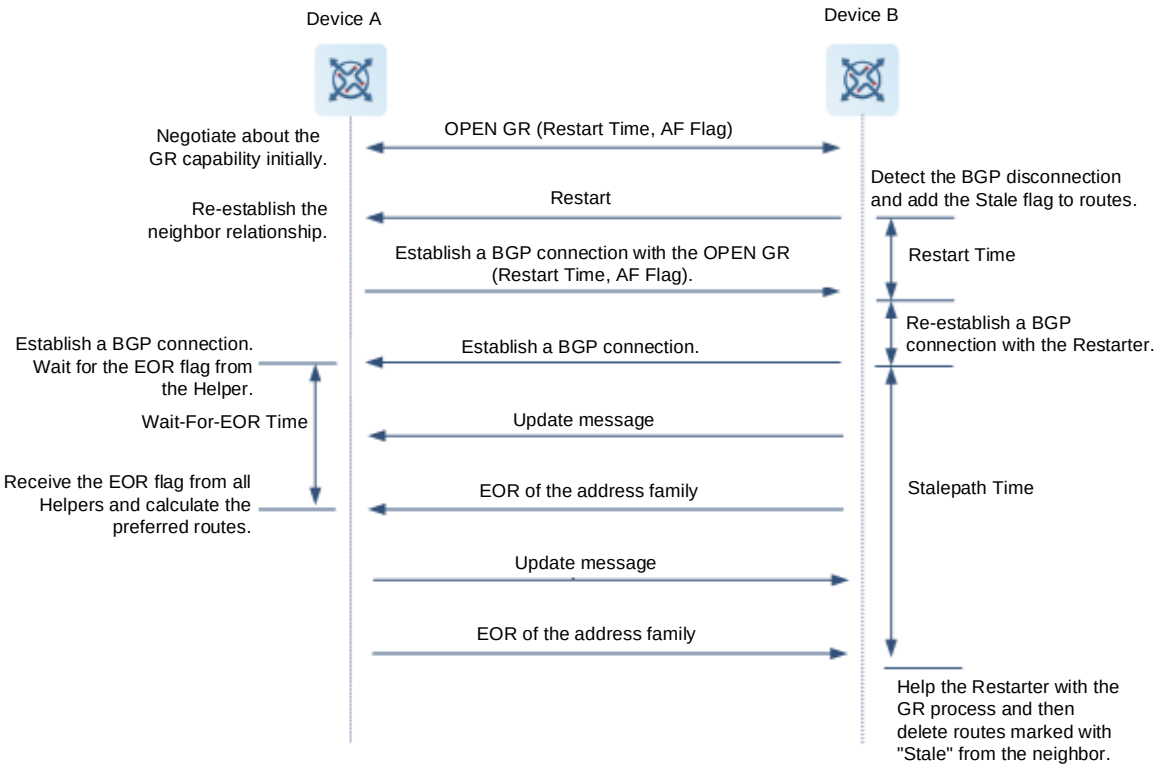
BGP GR is not an independent process, but is jointly accomplished by the Restarter and Helper.

- The Restarter performs restart and is capable of making the route forwarding plane to keep working when the route control plane is faulty.
- The Helper is the BGP neighbor of the Restarter and helps the Restarter complete GR.

To deliver graceful restart, BGP adds a capability field indicating to neighbors its support for GR to the OPEN message. The capability is called Graceful Restart Capability. During initialization of a BGP connection, both neighbors negotiate about the GR capability.

The End-of-RIB (EOR) flag is added to the update packets of BGP, to indicate that the routing information update to the neighbor is completed.

Figure 1-1 BGP GR Interaction Process



(1) When BGP establishes a neighbor relationship at the beginning, BGP uses the GR capability field in the OPEN message to negotiate about the GR capabilities of both neighbors.

(2) At a moment, the Restarter performs restart, and the BGP session is disconnected. The Helper detects the disconnection, keeps the route of the Restarter valid, but marks the Stale (aged but not updated).

(3) The Restarter completes restart.

(4) The Restarter connects to the Helper again.

(5) The Restarter waits for the route update message and EOR flag from the Helper.

(6) After receiving the EOR flag from all neighbors, the Restarter performs route calculation, updates routing entries, and then sends updated routes to the Helper.

(7) After receiving the updated routes, the Helper cancels their Stale flag. After receiving the EOR flag from the Restarter, the Helper deletes routes with the Stale flag (these routes are not updated), calculates routes calculation, and updates the routing entries. The entire GR process is completed.

BGP GR defines several important extended timers:

- **Restart-Timer**

  The value of this timer is advertised by the GR Restarter to the GR Helper. It indicates the maximum waiting time that the GR Restarter hopes the Helper to wait before a new connection is established between them. You can run the **bgp graceful-restart restart-time** command to change the time value.

- **Wait-For-EOR Timer**

This timer indicates the maximum time for the GR Restarter to wait for the EOR flag from all GR Helpers. After the EOR flag is received from all GR Helpers or the Wait-For-EOR timer expires, the GR Restarter calculates the preferred routes and updates the routing entries.

- **StalePath Timer**

  The timer indicates the maximum time for the GR-Helper to wait for the EOR flag from the GR Restarter after the connection between them is restored. Within this period, the Helper keeps the original route of the Restarter valid. After receiving the EOR flag or after the StalePath timer expires, the Helper clears the routing entries with the Stale tag. You can run the **bgp graceful-restart stalepath-time** command to change the time value.

2. BGP NSR

None-stop-routing (NSR) is used to ensure uninterrupted routes during protocol restart upon a switchover between the master and slave supervisor engines. During the switchover, the NSR function keeps the network topology stable, maintains the neighbor status and forwarding table, and ensures that key services are not interrupted.

Unlike BGP GR, BGP NSR does not need the assistance of neighbors.

- Connections between BGP neighbors are not interrupted during active/standby switchover.
- Neighbors do not perceive the restart behavior of the peer device. The GR technology is used for restart restoration.

Neighbors with the BGP NSR function enabled do not need to negotiate about the GR capability nor need assistance from the peer. Therefore, no interworking problem arises.

3. Fast rerouting

With the fast development of IP technologies and the application of various complex services, higher requirements are posed for network security and stability. Some real-time services (audios and videos) are sensitive to the network running status and are largely affected by unstable networks. Therefore, network reliability receives more and more attention. In response to this requirement, the IP Fast Reroute (FRR) function appears. This function aims to use a backup link to forward data during route platform convergence after a faulty link is detected so as to ensure that intact packets are forwarded timely.

Thus, BGP FRR can avoid route disconnection due to a link fault before BGP route convergence. If a BGP routing table has multiple paths to the same network, BGP calculates the route with the highest priority by default. After the BGP FRR function is used, BGP selects a backup route for each optimal route. When detecting a fault occurring on the master link by using the BFD fast link detection mechanism, the device switches data to the selected backup link for data forwarding. After route convergence is completed, the device switches data to the re-calculated optimal path for data forwarding.

1.1.12 BMP

BGP Monitor Protocol (BMP) monitors BGP running on a device. It focuses on the status of BGP peers, peer entry transmission and receiving, and all kinds of BGP peer statistics.

A BGP speaker proactively sends a TCP connection request to a specified BMP server. After a TCP connection is established successfully, the BGP speaker advertises a BMP packet to the BMP server. In the TCP connection request initiated by a BGP speaker to a BMP server, the destination IP address is the IP address of the specified BMP server and the port number is a specified port number.

1.1.13 Others

1. Regular expression

A regular expression matches strings based on a rule. It is used to assess text data and return True or False to decide whether the expression can correctly describe the data.

The following table describes special characters involved in regular expressions used in BGP path attributes.

Table 1-1 Description of Special Characters in a Regular Expression

Character	Symbol	Special Meaning
Period	.	Matches any single character.
Asterisk	*	Matches zero or any sequence in a string.
Plus sign	+	Matches one or any sequence in a string.
Question mark	?	Matches zero or one symbol in a string.
Caret	^	Matches the start of a string.
Dollar sign	$	Matches the end of a string.
Underline	_	Matches commas, brackets, start and end of a string, and spaces.
Square brackets	[ ]	Matches a single character within a range.

1.1.14 Protocols and Standards

- RFC 1105: Border Gateway Protocol (BGP)
- RFC 1163: Border Gateway Protocol (BGP)
- RFC 1267: Border Gateway Protocol 3 (BGP-3)
- RFC 1771: A Border Gateway Protocol 4 (BGP-4)
- RFC 4271: A Border Gateway Protocol 4 (BGP-4)
- RFC 4273: Definitions of Managed Objects for BGP-4
- RFC 4360: PrBGP Extended Communities Attribute
- RFC 4364: Proposed Standard: BGP/MPLS IP Virtual Private Networks (VPNs)
- RFC 4486: Proposed Standard: Subcodes for BGP Cease Notification Message
- RFC 4724: Proposed Standard: Graceful Restart Mechanism for BGP
- RFC 4760: Draft Standard: Multiprotocol Extensions for BGP-4
- RFC 4893: BGP Support for Four-octet AS Number Space
- RFC 5396: Textual Representation of Autonomous System (AS) Numbers
- RFC 5492: Draft Standard: Capabilities Advertisement with BGP-4
- RFC 6198: Requirements for the Graceful Shutdown of BGP Sessions

- RFC 7313: Enhanced Route Refresh Capability for BG: P-4
- RFC 7311: The Accumulated IGP Metric Attribute for BGP
- RFC 7432: Proposed Standard: BGP MPLS-based Ethernet VPN

1.2 Configuration Task Summary

BGP configuration includes the following tasks:

- Configuring BGP Basic Features
  - Configuring a BGP Neighbor
  - (Optional) Configuring a BGP IPv6 Address Family
  - (Optional) Configuring a BGP Peer Group
  - (Optional) Configuring the Dot Mode to Display 4-Byte AS Numbers
  - Configuring Routing Information Advertisement
  - (Optional) Configuring Multi-Path Route Import Between VRF Instances
  - (Optional) Shutting Down BGP Connections Gracefully
  - (Optional) Configuring BGP Soft Reset
  - (Optional) Configuring Route Update Mechanisms of BGP
  - (Optional) Configuring BGP Capacity Protection
- (Optional) Configuring a large BGP Network. All the following configuration tasks are optional and may be selected as needed.
  - Configuring a Route Reflector
  - Configuring an AS Alliance
  - Configuring Route Aggregation
  - Configuring Route Dampening
- (Optional) Configuring BGP Route Selection and Load Balancing. All the following configuration tasks are optional and may be selected as needed.
  - Configuring Multi-path Load Balancing of BGP
  - Configuring BGP Routes to Be Recursive Only to Host Routes
  - Configuring Outbound Loop Detection for a BGP Neighbor
  - Configuring BGP ADD-PATH
  - Configuring BGP to Advertise Routes with the Lowest Priority upon Device Restart
  - Configuring the AS_PATH Attribute
- (Optional) Configuring BGP to Control Route Advertisement and Receiving. All the following configuration tasks are optional and may be selected as needed.
  - Configuring Fast Withdrawal of Specified BGP Routes
  - Configuring Delayed Route Advertisement of BGP
- (Optional) Configuring the BGP Security Function. All the following configuration tasks are optional and may be selected as needed.

  - Configuring MD5 Authentication
  - Configuring the Generalized TTL Security Mechanism (GTSM) Security Check for BGP Neighbors
- (Optional) Configuring BGP Reliability. All the following configuration tasks are optional and may be selected as needed.
  - Configuring BFD For BGP
  - Configuring BGP FRR
  - Configuring EBGP Multi-Path Bypass Protection
  - Configuring BGP GR
  - Configuring BGP NSR
  - Configuring BGP Session Retention
- (Optional) Enabling the Extended Functions of BGP. All the following configuration tasks are optional and may be selected as needed.
  - Configuring BMP Monitoring
  - Configuring the Administrative Distance of BGP

1.3 Configuring BGP Basic Features

1.3.1 Configuration Tasks

The configuration of BGP basic features includes the following tasks:

- Configuring a BGP Neighbor
- (Optional) Configuring a BGP IPv6 Address Family
- (Optional) Configuring a BGP Peer Group
- (Optional) Configuring the Dot Mode to Display 4-Byte AS Numbers
- Configuring Routing Information Advertisement
- (Optional) Configuring Multi-Path Route Import Between VRF Instances
- (Optional) Shutting Down BGP Connections Gracefully
- (Optional) Configuring BGP Soft Reset
- (Optional) Configuring Route Update Mechanisms of BGP
- (Optional) Configuring BGP Capacity Protection

1.3.2 Configuring a BGP Neighbor

1. Overview

This section describes how to configure a BGP speaker as a neighbor.

2. Restrictions and Guidelines

- If IBGP neighbors are not directly connected, you need to configure IGP or a static routing protocol to implement reachable routes between the neighbors.
- If EBGP neighbors are not directly connected, you need to configure the **ebgp-multihop** parameter for the neighbors.

- The source interface for establishing a neighbor relationship must be a valid local interface or IP address.
- You can run the **exit-address-family** command to exit the address family configuration mode of BGP.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) (Optional) Enter a required address family configuration mode. If you need to perform configuration for a specific address family, select one of the following tasks to configure.

- Enter the IPv4 unicast configuration mode.

  address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(5) Create a BGP neighbor. When the configured AS number is the same as the local AS number, an IBGP neighbor is created. When the configured AS number is different from the local AS number, an EBGP neighbor is created.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

No neighbor is specified for a BGP speaker by default.

(6) (Optional) Configure a source interface or IP address for establishing a TCP connection with the neighbor. A loopback interface is recommended for IBGP neighbors while a directly connected interface is recommended for EBGP neighbors.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **update-source** { *interface-type interface-number* | *address* }

BGP automatically selects the source IP address for a TCP connection based on the IP address of a neighbor by default. The IP address of the outbound interface of local packets is generally used.

(7) (Optional) Configure the time to live (TTL) for TCL packets received from the neighbor. A larger TTL value indicates more hops to the neighbor. When the TTL is **1**, the BGP neighbor must be directly connected to the device.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **ebgp-multihop** [*ttl*]

The default TTL values of TCP packets to be sent to IBGP neighbors and EBGP neighbors are **255** and **1** respectively.

(8) (Optional) Configure the mode for BGP to establish a TCP connection with the neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **transport connection-mode** { **active-only** | **both** | **passive-only** }

By default, BGP neighbors support the active and passive modes of establishing TCP connections.

(9) (Optional) Activate the address family capability for the neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **activate**

Only the IPv4 unicast address family capability is activated for neighbors created in BGP configuration mode by default.

1.3.3 Configuring a BGP IPv6 Address Family

1. Overview

This section describes how to configure BGP to exchange IPv6 routes to implement IPv6 network access between different ASs.

2. Restrictions and Guidelines

- Generally, BGP uses IPv6 addresses to establish neighbor relationships and implement the exchange of IPv6 routes.
- In special scenarios, for example, the IPv6 provider edge router (6PE) function is configured, BGP supports the exchange of IPv6 routes with the neighbors using IPv4 addresses.
- Configurations related to BGP IPv6 services must be completed in BGP IPv6 address family mode.
- Neighbors using IPv6 addresses are used to exchange IPv6 routes. When a neighbor is configured in BGP mode, BGP automatically activates the IPv4 unicast address family capability for the neighbor. You are advised to manually disable the IPv4 unicast address family capability.
- You can run the **exit-address-family** command to exit the address family configuration mode of BGP.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(5) Configure the BGP IPv4 address family mode.

address-family ipv4 unicast

(6) Disable the IPv4 address family capability for the BGP neighbor.

no neighbor { *neighbor-ipv4-address* | *peer-group-name* } **activate**

The IPv4 address family capability is enabled by default.

(7) Configure the BGP IPv6 address family mode.

address-family ipv6 unicast

(8) Configure the IPv6 address family capability for the BGP neighbor.

neighbor { *neighbor-ipv6-address* | *peer-group-name* } **activate**

The IPv6 address family capability is disabled by default.

(9) (Optional) Configure BGP to advertise IPv6 routes.

network *network-ipv6-address/prefix-length* [**route-map** *route-map-name*] [**backdoor**]

No network routing information is configured for BGP by default.

1.3.4 Configuring a BGP Peer Group

1. Overview

BGP speakers in the same peer group have the same update strategy. Peer groups can simplify configuration and improve the running efficiency.

2. Restrictions and Guidelines

- Members of a peer group inherit all configurations of the peer group. Unified configuration of a peer group can be replaced by separate configuration of each member in the peer group, except the configuration that influences output update, for example, the configuration of neighbor distribute-list, neighbor route-map, and neighbor filter-list.
- You can neither put neighbors belonging to different address families to the same peer group nor put IBGP and EBGP neighbors to the same peer group.
- You can run the **exit-address-family** command to exit the address family configuration mode of BGP.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) (Optional) Enter a required address family configuration mode. If you need to perform configuration for a specific address family, select one of the following tasks to configure.

Enter the IPv4 unicast configuration mode.

address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(5) Create a peer group.

neighbor *peer-group-name* **peer-group**

(6) Specify a BGP speaker as a member of the BGP peer group.

neighbor { neighbor-ipv4-address | neighbor-ipv6-address } **peer-group** *peer-group-name*

1.3.5 Configuring the Dot Mode to Display 4-Byte AS Numbers

1. Overview

The 4-byte AS numbers can be represented in dot mode.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure the dot mode to display 4-byte BGP AS numbers.

bgp asnotation dot

1.3.6 Configuring Routing Information Advertisement

1. Overview

This section describes how to configure network information to be advertised by the local BGP speaker. Network information to be advertised can be direct routes, static routes, and dynamic routes.

2. Restrictions and Guidelines

- You are advised to enable the network information synchronization function. Otherwise, routing black holes may be incurred.
- You can run the **exit-address-family** command to exit the address family configuration mode of BGP.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) (Optional) Enter a required address family configuration mode. If you need to perform configuration for a specific address family, select one of the following tasks to configure.

- Enter the IPv4 unicast configuration mode.

  address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(5) Add static routing entries to a BGP routing table and advertise the routing entries to peers.

network *network-number* [**mask** *mask*] [**route-map** *route-map-name*] [**backdoor**]

No static routing entry is added to a BGP routing table and advertised to peers by default.

(6) (Optional) Configure a device to advertise routing information configured by running the **network** command after the device synchronizes with the local route.

network synchronization

By default, a device will advertise routing information configured by running the **network** command after the device synchronizes with the local route.

1.3.7 Configuring Multi-Path Route Import Between VRF Instances

1. Overview

This section describes how to configure multi-path route import between VRF instances. Routes imported between VRF instances form multiple ECMP paths.

2. Restrictions and Guidelines

- This command does not allow IBGP and EBGP routes to form equivalent routes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure a BGP VRF address family.

(5) Enter a required address family configuration mode. If you need to perform configuration for a specific address family, select one of the following tasks to configure.

- Enter the IPv4 unicast configuration mode.

  address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(6) Configure route re-distribution to re-distribute IGP routes to BGP.

redistribute *protocol-type* [**route-map** *route-map-name*] [**metric** *metric-value*]

The route re-distribution function is disabled by default.

(7) (Optional) Configure route re-distribution to re-distribute only IBGP routes to IGP.

bgp redistribute-internal

Routes learned from IBGP can be re-distributed to IGP by default.

(8) Enable the function of importing multiple next-hop routes from other protocols to BGP.

bgp sourced-paths *protocol-type* **all**

The function of importing multiple next-hop routes is disabled by default.

(9) Configure BGP ECMP multi-path load balancing.

maximum-paths { **ebgp** | **ibgp** } *maximum-path-number*

The ECMP function is disabled by default.

(10) Configure the import of routes of all paths between VRF instances, to control the import of all next-hop routes, preferred next-hop routes, or equal-cost next-hop routes.

import path selection { **all** | **bestpath** | **multipath** }

Only preferred next-hop routes are imported by default.

When routes are imported into a virtual routing and forwarding (VRF) instance, only routes with preferred next hops are imported. The enhanced VPN route import function extends the import of the preceding routes, and supports the import of all next-hop routes or equal-cost next-hop routes.

1.3.8 Shutting Down BGP Connections Gracefully

1. Overview

In a network, as a user isolates or upgrades a device, the RFC 6198 defines a function of shutting down BGP connections gracefully. This function demands the device to shut down connections with its neighbors when service traffic is not interrupted or is interrupted for a short time.

This feature adopts the "Make-Before-Break" mode to shut down BGP connections, to ensure that service traffic is not interrupted or is interrupted for a very short period of time in the process from the feature configuration to actual BGP connection shutdown. The steps are as follows:

(1) The feature enables the device to advertise a route with the lowest priority (the value of Local-Pref is **0** or the value of MED is 4,294,967,295), carrying Gshut Community, to a neighbor. Then, the neighbor updates the route and switches traffic to a backup link or other equal-cost links.

(2) The device shuts down the BGP connection with the neighbor after a period of time.

The delay time for BGP connection shutdown can be manually specified or automatically calculated. The automatically calculated delay time is based on 1 second for 1,000 routes.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Shut down all connections in a BGP instance gracefully.

bgp shutdown graceful [**community** *community-value*] [**delay** *delay-time*]

None of the connections in a BGP instance is shut down by default.

(5) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(6) Shut down connections of the BGP neighbor gracefully.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **shutdown graceful** [**community** *value*] [**delay** *time*]

None of the connections of a BGP neighbor is shut down by default.

1.3.9 Configuring BGP Soft Reset

1. Overview

If routing policies (including neighbor distribute-list, neighbor route-map, neighbor prefix-list, and neighbor filter-list) are modified, an effective method must be available to implement new routing policies. The conventional method is to configure BGP soft reset, which implements a new routing policy without terminating a BGP session connection. When an output routing policy is modified, BGP soft reset will re-advertise all routing information of a BGP speaker to its neighbors.

If an input routing policy is modified, the operation is more complex than that performed when an output routing policy is modified. This is because output routing policies are implemented on the routing table of the local BGP speaker, while the input routing policies are implemented on the routing information received from BGP peers. The local BGP speaker does not retain the original routing information received from BGP peers to reduce memory occupancy. If an input routing policy is modified and a neighbor supports the route update function, you can configure soft reset to send a route update request to the neighbor. After receiving the request, the neighbor re-advertises all routing information. You can also configure the local BGP speaker to store original routing information for each specified BGP peer and the original routing information is used as a basis for judging the modification of input routing policies.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Clear the specified session of the BGP IPv4 unicast address family.

clear bgp ipv4 unicast [**vrf** vrf-name] { ***** | *as-number* | *neighbor-ipv4-address* | *neighbor-ipv6-address* } **soft**]**out**

(3) Enter the global configuration mode.

configure terminal

(4) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(5) (Optional) Save the original routing information of a specified BGP peer.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

No original routing information of a specified BGP peer is saved by default.

1.3.10 Configuring Route Update Mechanisms of BGP

1. Overview

BGP provides two route update mechanisms: regular scanning update and event triggering update.

- Regular scanning update

  BGP uses an internal timer to start scanning regularly and update the routing table.

- Event triggering update

  When BGP configuration commands are changed due to user configuration or the next hop of a BGP route changes, BGP is triggered to start the scanning mechanism and update the routing table.

  The function of triggering routing table update by the change of the next hop of BGP is a method of reducing the BGP convergence time. This function optimizes the method of monitoring the next hops of routes, to enable BGP to speed up route convergence when the network topology is stable. When BGP establishes a connection with a neighbor, it automatically monitors the next hops of the routes learned from the neighbor. When a next hop changes in the core routing table, BGP receives a next hop change advertisement and updates the BGP routing table. This optimization measure improves the convergence performance of BGP routes by reducing the time for detecting next-hop changes.

2. Restrictions and Guidelines

- Based on address families, this function is configured in the IPv4, IPv6, IPv4 VRF, and IPv6 VRF address family modes.
- If you set the BGP route update mechanism to event-triggering update, you must disable synchronization (by running the **no synchronization** command) and enable the BGP next-hop triggering update function. Otherwise, you must not configure such update.
- The **bgp nexthop trigger delay** command and the **bgp scan-time** command control the same timer. If the BGP route update mechanism is configured as regular scanning update and the timer specified in the **bgp nexthop trigger delay** command is set to greater than 60 seconds, this command does not take effect, because the scanning timer is triggered prior to the delay of the next hop triggering update.
- In an unstable network environment with frequent hop changes, especially with many routes, the configuration of the next hop triggering update causes unnecessary route calculations, and thus consumes more CPU resources. Therefore, you are advised to disable this function in this environment.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure an interval of regular scanning update of BGP.

bgp scan-time *scan-time*

The default interval of regular scanning update of BGP is **60** seconds.

(5) (Optional) Enter the address family configuration mode. To configure this function for a specific address family, please configure only one task.

- Enter the IPv4 unicast configuration mode.

  address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(6) Configure the BGP route update mechanism as event triggering update. Run the following commands in turn:

- Configure the event triggering update mechanism to update the routing table.

  bgp scan-rib disable

  BGP updates the routing table in regular scanning mode by default.

- Enable the next hop triggering update.

  bgp nexthop trigger enable

  The function of next hop triggering update is enabled by default.

- Configure a delay of updating the routing table before the next hop of a BGP route changes.

  bgp nexthop trigger delay *delay-time*

  The default delay of updating the routing table is **5** seconds after the next hop of a BGP route changes.

1.3.11 Configuring BGP Capacity Protection

1. Overview

Excessive BGP routing entries can overload the device capacity, especially on devices with a small memory. BGP capacity protection can help avoid non-predictable running status caused by excessive resource consumption of the device.

- Restricting the number of BGP routing entries

  The number of BGP routing entries is restricted by configuring the maximum number of routing entries in a BGP address family and the maximum number of routing entries that are learned by a BGP neighbor.

- Enabling BGP to enter the overflow state in case of memory insufficiency

  BGP is allowed to enter the overflow state when the memory is insufficient. In the overflow state, BGP generates a default route pointing to the null interface. If a newly learned route is not a refined route of a non-default route in the current routing table, the route is discarded. The system memory is kept stable by

discarding eligible routes. The purpose of only discarding routes meeting specific conditions is to prevent route loops in the network. Therefore, BGP in the overflow state is secure.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure BGP to enter the overflow state when the memory is insufficient.

overflow memory-lack

BGP enters the overflow state by default when the memory is insufficient.

(5) Enable the function of route entry limit in global configuration mode or for specified VRF instances.

bgp maximum-prefix *maximum-prefix-numbers* [**vrf** *vrf-name*]

The function of route entry limit is disabled in global configuration mode or for specified VRF instances by default.

(6) Configure the maximum number of prefixes received from specified BGP peers.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **maximum-prefix** *maximum-prefix-value* [*maximum-prefixthreshold*] [**restart-time** *restart-time* | **warning-only** [**suppress**]]

The number of prefixes received from a specified BGP peer is not limited by default.

(7) (Optional) Enter the address family configuration mode. To configure this function for a specific address family, please configure only one task.

- Enter the IPv4 unicast configuration mode.

  address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(8) Configure the maximum number of prefixes in a BGP routing information base under the address family.

maximum-prefix *maximum-prefix-number*

The number of route prefixes in a BGP routing information base under an address family is not limited by default.

1.4 Configuring a large BGP Network

1.4.1 Configuration Tasks

The large BGP network configuration includes the following tasks: All configuration tasks are optional and may be selected as needed.

- Configuring a Route Reflector
- Configuring an AS Alliance
- Configuring Route Aggregation
- Configuring Route Dampening

1.4.2 Configuring a Route Reflector

1. Overview

A route reflector can be configured in an IBGP environment so that routing information is reflected between clients and the number of BGP neighbor connections is reduced.

2. Restrictions and Guidelines

- If you configure a route reflector in an address family, the reflector takes effect only in this address family.
- To facilitate configuration, you need to configure the reflector device. The client devices do not need to be configured as clients.
- When multiple reflection clusters are deployed in one AS domain, different reflection cluster identifiers must be configured for them.
- You can run the **exit-address-family** command to exit the address family configuration mode of BGP.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(5) Configure the local device as a route reflector. Then, the BGP neighbor becomes the route reflection client.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **route-reflector-client**

(6) (Optional) Enable the route reflection function between clients of the devices.

bgp client-to-client reflection

The route reflection function between clients is enabled by default.

(7) (Optional) Configure a BGP reflection cluster ID.

bgp cluster-id *cluster-id*

A BGP reflection cluster ID is the BGP router-ID by default.

(8) (Optional) Allow the BGP route reflector to modify route attributes.

bgp route-reflector attribute-change

No route reflector is allowed to modify route attributes by default.

According to RFC4456, to prevent route loops, a BGP route reflector cannot modify route attributes when reflecting routes. However, relevant route attributes need to be modified when you re-plan network traffic paths. Users can configure a command to modify route attributes (including Route-map and Nexthop-self) on the route reflector.

1.4.3 Configuring an AS Alliance

1. Overview

On a large BGP network, you can configure a BGP alliance to divide an AS into multiple member ASs, to reduce the number of IBGP neighbor connections and facilitate AS management.

2. Restrictions and Guidelines

- You are advised to use private AS numbers for member ASs within an alliance. A private AS number is in the range from 64512 to 65535.
- Within a member AS of an alliance, BGP speakers must be connected in a full mesh manner or configured as reflectors and reflector clients.
- EBGP neighbor relationships must be established between member ASs of an alliance.
- All BGP speakers in an alliance must associate with a member AS of the alliance.
- All member ASs that have established EBGP relationships with the local device must be configured on members of a BGP alliance.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure a BGP alliance ID. The local BGP AS (specified by the **router bgp** *as-number* command) becomes the private AS inside the alliance and is invisible to other AS domains.

bgp confederation identifier *as-number*

No alliance ID is configured for a BGP speaker by default.

(5) Configure members for the BGP alliance. The specified AS and local AS belong to the same alliance.

bgp confederation peers *as-number*&<1-n>

No alliance member is configured for BGP by default.

1.4.4 Configuring Route Aggregation

1. Overview

One or more refined BGP routes are aggregated as a BGP route with a shorter network mask.

2. Restrictions and Guidelines

- By default, BGP advertises path information before and after aggregation. To enable BGP to advertise only path information after aggregation, run the **aggregate-address summary-only** command.
- When the **aggregate-address** command is used to configure route aggregation, the aggregated routes take effect immediately as long as any route falls into the configured address range.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure the route aggregation entries of BGP.

aggregate-address { *ipv4-address mask* | *prefix* } [**advertise-map** route-map-name | **as-set** | **attribute-map** *route-map-name* | **summary-only** | **suppress-map** route-map-name] *

No route aggregation entry of BGP is configured by default.

1.4.5 Configuring Route Dampening

1. Overview

BGP route dampening is a method of reducing route flapping. It reduces possible route flapping by monitoring routing information from EBGP peers. The BGP speaker punishes a route once (added to the penalty) route flapping occurs. When the penalty reaches the upper limit, the route is suppressed. When the Half-life-time reaches, the penalty is halved. When the penalty is reduced to the Reuse Limit, the route is reactivated.

2. Procedure

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Enable the route dampening function and configure dampening parameters.

bgp dampening [*half-life* [*reusing suppressing maximun-supress-time*] [**withdrawal-ignore**] | **route-map** *route-map-name*]

The route dampening function is disabled by default.

1.5 Configuring BGP Route Selection and Load Balancing

1.5.1 Configuration Tasks

The configuration of BGP route selection and load balancing includes the following tasks: All configuration tasks are optional and may be selected as needed.

- Configuring Multi-path Load Balancing of BGP
- Configuring BGP Routes to Be Recursive Only to Host Routes
- Configuring Outbound Loop Detection for a BGP Neighbor
- Configuring BGP ADD-PATH
- Configuring BGP to Advertise Routes with the Lowest Priority upon Device Restart
- Configuring the AS_PATH Attribute

1.5.2 Configuring Multi-path Load Balancing of BGP

1. Overview

This section describes how to implement multi-path load balancing for IBGP routes.

2. Restrictions and Guidelines

- Routes learned from an IBGP neighbor must have the same priority (the router-ID is not compared).
- This command does not allow IBGP and EBGP routes to form equivalent routes.
- All next hops must carry the Link-Bandwidth attribute so that non-equal-cost routes are generated. Otherwise, non-equal-cost load balancing cannot be implemented.
- Enable the function of sending extended community attributes so that the link bandwidth attribute can be sent to an IBGP neighbor.
- The function of carrying the link bandwidth attribute when a route from a specified neighbor is sent to an IBGP neighbor takes effect only on single-hop EBGP neighbors.
- You can run the **exit-address-family** command to exit the address family configuration mode of BGP.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) (Optional) Enter a required address family configuration mode. If you need to perform configuration for a specific address family, select one of the following tasks to configure.

- Enter the IPv4 unicast configuration mode.

  address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(5) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(6) Configure BGP load balancing. To configure equal-cost route load balancing by EBGP multiple paths of an alliance or by local inter-VRF imported routes, run the **maximum-paths ebgp** command.

maximum-paths { **ebgp** | **ibgp** } *maximum-paths-number*

BGP load balancing is disabled by default.

(7) (Optional) Configure the AS-PATH loose comparison mode, in which only the AS-PATH length is compared.

bgp bestpath as-path multipath-relax

The AS-PATH exact comparison mode is used by default, in which the AS-PATH attribute must be exactly the same when BGP calculates multiple equal-cost paths.

(8) (Optional) Enable the function of sending extended community attributes, to ensure that the link bandwidth attribute is transferred between neighbors.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **send-community** [**both** | **standard** | **extended**]

The function of advertising community attributes to a specified BGP neighbor is not configured by default.

(9) (Optional) Enable non-equal-cost load balancing. Non-equal-cost routes are generated based on the link bandwidth attribute.

bgp dmzlink-bw

Non-equal-cost load balancing is disabled by default.

(10) (Optional) Enable the function of carrying the link bandwidth attribute when a route from a specified neighbor is sent to an IBGP neighbor.

neighbor { *peer-address* | *peer-group-name* } **dmzlink-bw**

The function of carrying the link bandwidth attribute in a route from a specified neighbor is disabled by default.

1.5.3 Configuring BGP Routes to Be Recursive Only to Host Routes

1. Overview

BGP routes use optimal matching for route recursion by default. BGP routes may be recursive to default routes or incorrect network segment routes, resulting in an error in the egress or next hop. After the function of making BGP routes recursive only to host routes is enabled, BGP routes are recursive only to 32-bit IPv4 host routes or 128-bit IPv6 host routes. This function is applied to routes learned by IBGP neighbors or multi-hop EBGP neighbors that have established neighbor relationships by using the loopback interface.

After the function of making BGP routes recursive only to host routes is enabled, the device checks the validity of the next-hop addresses of IBGP or multi-hop EBGP routes via exact matching, and conducts route recursion on the IBGP or multi-hop EBGP routes via exact matching when they are written into the forward information database (FIB). For example, the next-hop address of the IBGP route 192.168.2.0/24 is 1.1.1.1. The next-hop address of the IBGP route 192.168.2.0/24 is valid only when the route 1.1.1.1/32 exists, and the egress of the route written into the FIB is the egress of the route 1.1.1.1/32.

2. Restrictions and Guidelines

- This function takes effect only on IBGP or multi-hop EBGP routes. It is unavailable to direct EBGP routes or routes whose next-hop addresses are direct connection addresses.
- IBGP or multi-hop EBGP neighbor relationships of the device need to be established using the address of the loopback interface. Otherwise, this function cannot be enabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure BGP routes to be recursive only to host routes.

bgp recursion host

BGP routes recurse via optimal matching by default.

1.5.4 Configuring Outbound Loop Detection for a BGP Neighbor

1. Overview

When receiving a BGP route from a neighbor, BGP conducts loop detection on the BGP route by default. If the AS-PATH attribute carried in a BGP route contains the local AS number, BGP filters out the BGP route. The BGP outbound loop detection is to conduct loop detection on routes before the routes are transmitted to a neighbor, so as to filter out loop routes.

When sending a route to an EBGP neighbor, the device judges whether the AS-PATH attribute carried in the BGP route contains the AS number of the neighbor. If yes, the route is looped and the device does not send the route to the EBGP neighbor.

2. Restrictions and Guidelines

This feature is available only to EBGP neighbors.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(5) Configure outbound loop detection for the BGP neighbor

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **as-loop-check out**

The outbound loop detection is disabled for a neighbor by default.

1.5.5 Configuring BGP ADD-PATH

1. Overview

The BGP additional paths (ADD-PATH) attribute is used to receive multiple routes with the same prefix from an IBGP neighbor. When receiving routes with the same prefix from the same peer, BGP replaces a previous route with the latest new one by default, that is, BGP regards the routes with the same prefix received from the same neighbor as one entry. After the BGP ADD-PATH function is configured, BGP adds a path-ID field to the route advertised to a neighbor that supports the ADD-PATH capability. The device judges whether routes are the same based on the route prefix and path-ID of a neighbor. When a received route is different from previous routes, the device adds it as a new entry. In this way, the device can obtain multiple routes with the same prefix from the same neighbor.

2. Restrictions and Guidelines

Run the **bgp additional-paths select** command to select ADD-PATH alternative routes of a specific type. If the type of selected ADD-PATH alternative routes is different from that of to-be-advertised ones, the ADD-PATH alternative routes are not advertised but only the optimal routes are advertised.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Enable the ADD-PATH selection function.

bgp additional-paths select { **all** | **best** *number* | **ecmp** }

(5) Create a BGP neighbor.

neighbor { neighbor-ipv4-address | neighbor-ipv6-address | peer-group-name } **remote-as** as-number

(6) The ADD-PATH function is disabled by default. Configure the device to advertise the ADD-PATH alternative routes of a specific type to a peer when the ADD-PATH negotiation is successful.

neighbor { *peer-address* | *peer-group-name* } **advertise additional-paths** { **all** | **best** *number* | **ecmp** }

BGP does not advertise ADD-PATH alternative routes to its neighbors by default.

(7) Enable the ADD-PATH capability for a specified peer.

neighbor { *peer-address* | *peer-group-name* } **additional-paths** { **send [receive] | receive** }

The ADD-PATH capability of a peer is disabled by default.

1.5.6 Configuring BGP to Advertise Routes with the Lowest Priority upon Device Restart

1. Overview

By default, after a neighbor relationship is established upon device restart, a BGP peer can advertise routes to its neighbors. However, in certain cases, for example, a device has many neighbors, there are considerable routes during device startup, but writing entries into the hardware is slow. The neighbors have learned the routes and started forwarding traffic, but the local device has not completed the writing of entries into the hardware, causing a traffic forwarding failure. Therefore, it is necessary to adjust the priority of routes advertised by BGP to the lowest priority after the device restart. In this way, routes passing through the local device are not selected while other routes are available.

This function enables BGP to advertise routes with the lowest priority to neighbors after the local device is started and has established a neighbor relationship. For EBGP neighbors, the MED value of routes is adjusted to **4294967295**. For IBGP neighbors, the LOCAL_PREF value of routes is adjusted to **0**. After confirming that ARP entries have been delivered and forwarding entries have been written into hardware, run the **clear bgp advertise lowest-priority on-startup** command to restore the priority of advertised routes. If you do not configure the priority restoration for advertised routes, the device automatically restores the priority of advertised routes after a period of time.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure BGP to adjust the priority of advertised routes to the lowest level upon device restart.

bgp advertise lowest-priority on-startup [*recover-time*]

BGP does not modify the priority of advertised routes by default.

1.5.7 Configuring the AS_PATH Attribute

1. Overview

AS_PATH Lists the ASs passed by a route reversely. Routes are selected based on different AS_PATH attributes.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) (Optional) Enter the address family configuration mode. To configure this function for a specific address family, please configure only one task.

- Enter the IPv4 unicast configuration mode.

  address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(5) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(6) Configure the local AS for the BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **local-as** *as-number* [**no-prepend** [**replace-as** [**dual-as**]]]

No local AS is configured for any peer by default, and the local AS of a peer is the real AS of BGP.

After the local AS function is configured, when the real AS of the local BGP changes, you do not need to change the BGP configuration on the peer and a BGP connection can be still established. This function is used for AS migration and merging on large networks and ensures that the device configurations in other interconnected ASs are not affected.

1.6 Configuring BGP to Control Route Advertisement and Receiving

1.6.1 Configuration Tasks

The configuration of route advertisement and receiving control of BGP includes the following tasks: All configuration tasks are optional and may be selected as needed.

- Configuring Fast Withdrawal of Specified BGP Routes
- Configuring Delayed Route Advertisement of BGP

1.6.2 Configuring Fast Withdrawal of Specified BGP Routes

1. Overview

With the rapid development of IP technologies and the application of various complex services, higher requirements are posed for the network. Customers may need fast convergence of specific routes. This function can meet customers' requirements for preferential withdrawal of specific routes.

The route withdrawal sequence is calculated based on the routes in the routing table by default. This function adds routes that meet conditions to a high-priority queue for preferential processing, so as to achieve the purpose of rapidly withdrawing specified routes.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) (Optional) Enter the address family configuration mode. To configure this function for a specific address family, please configure only one task.

- Enter the IPv4 unicast configuration mode.

  address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(5) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(6) Configure BGP to rapidly withdraw specified routes.

bgp fast-withdraw { **access-list** { *access-list-number* | *access-list-name* } | **prefix-list** *prefix-list-name* | **route-map** *route-map-name* }

The rapid withdrawal of specified routes is disabled by default.

1.6.3 Configuring Delayed Route Advertisement of BGP

1. Overview

- Delayed advertisement upon system restart

  After the system is restarted and a neighbor relationship is established, a BGP peer can advertise routes to its neighbors. However, in certain cases, for example, a device has many neighbors or routes and the device is restarted. So, the device is slow in writing entries to hardware. As a result, the neighbors have learned the routes and started forwarding traffic, but the local device hardware has not completed writing of entries, causing a traffic forwarding failure.

  The BGP delayed advertisement upon system restart enables the device not to immediately advertise routes to its neighbors but wait for a period of time after the system is restarted and the BGP neighbor relationships are established. This function does not affect other behaviors of neighbors such as route receiving. If some routes need to be kept from impact of the system delay, you can configure a prefix-list policy to match these routes, providing a flexible route advertisement method.

  Delay-time specifies the waiting time before routes are advertised to neighbors and startup-time specifies the startup-time. Within the startup-time, BGP sends received routing information to the neighbors at an

interval specified by delay-time. After the startup-time ends, the default route advertisement behavior recovers.

- Delayed first route advertisement

  Once the neighbors of BGP negotiate to reach the established status, they send update packets each other. If delayed first route advertisement of BGP is configured on the local device, the local device will send the route received from the specified neighbor to other neighbors after the delayed period.

2. Restrictions and Guidelines

- If delayed advertisement of BGP upon system restart and delayed first route advertisement of BGP are enabled at the same time, delayed advertisement of BGP upon system restart takes precedence over delayed first route advertisement for first routes of BGP.
- BGP GR is not affected by either delayed advertisement of BGP upon system restart or delayed first route advertisement of BGP, that is, the BGP GR route advertisement is not affected by the delay time.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Enable the function of delayed advertisement of BGP upon system restart.

bgp initial-advertise-delay { *delay-time* [*startup-time*] [**wait-for-controller**] | **prefix-list** *prefix-list-name* }

The function of delayed advertisement of BGP upon system restart is disabled by default.

1.7 Configuring the BGP Security Function

1.7.1 Overview

The configuration of the BGP security function includes the following tasks: All configurations are optional and may be selected as needed.

- Configuring MD5 Authentication
- Configuring the Generalized TTL Security Mechanism (GTSM) Security Check for BGP Neighbors

1.7.2 Configuring MD5 Authentication

1. Overview

Message-digest algorithm 5 (MD5) authentication passwords are used when BGP speakers establish a TCP connection. If the authentication fails, no TCP connection will be established.

2. Restrictions and Guidelines

- The same password must be set for the BGP speakers that need to establish a BGP connection. Otherwise, no neighbor relationship can be established between them.

- After the MD5 authentication command is configured, BGP speakers re-establishes a BGP connection.
- Only one authentication password can be configured for one neighbor.
- You can run the **exit-address-family** command to exit the address family configuration mode of BGP.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) (Optional) Enter the address family configuration mode. To configure this function for a specific address family, please configure only one task.

- Enter the IPv4 unicast configuration mode.

  address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(5) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(6) Configure MD5 encryption for a TCP connection to be established with the BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **password** [**0** | **7**] *password-string*

By default, a BGP connection is not encrypted through MD5.

1.7.3 Configuring the Generalized TTL Security Mechanism (GTSM) Security Check for BGP Neighbors

1. Overview

Network devices consume CPU resources when processing IP packets on the control plane. An attacker continuously sends false BGP packets to a device. If the device finds the packets sent to the local device upon receipt of them and forwards the packets to the control plane for processing without identification, the device consumes many CPU resources, because it needs to process these packets.

Configuring BGP GTSM security check can protect devices from CPU type attacks. GTSM security check determines whether the TTL value in IP packet headers is within the specified range. If not, the packets are invalid and directly discarded.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure the function of GTSM security check for BGP neighbors.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **ttl-security hops** *hop-count*

The function of GTSM security check is not enabled by default.

1.8 Configuring BGP Reliability

1.8.1 Configuration Tasks

BGP reliability configuration includes the following tasks: All configurations are optional and may be selected as needed.

- Configuring BFD For BGP
- Configuring BGP FRR
- Configuring EBGP Multi-Path Bypass Protection
- Configuring BGP GR
- Configuring BGP NSR
- Configuring BGP Session Retention

1.8.2 Configuring BFD For BGP

1. Overview

You can configure bidirectional forwarding detection (BFD) for BGP to rapidly detect a network failure and switch data to a backup link, thereby improving the network use experience.

2. Restrictions and Guidelines

You can run the **exit-address-family** command to exit the address family configuration mode of BGP.

3. Prerequisites

Before configuring BFD for BGP, ensure that BFD session parameters have been configured for a relevant interface of a neighbor.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) (Optional) Enter the address family configuration mode. To configure this function for a specific address family, please configure only one task.

- Enter the IPv4 unicast configuration mode.

  address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(5) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(6) Configure BFD for BGP to detect the neighbor changes.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **fall-over bfd**

The BFD function is disabled by default.

1.8.3 Configuring BGP FRR

1. Overview

This section describes how to use a backup route to replace a failed route to rectify the fault locally.

2. Prerequisites

Configure a BFD session for a neighbor to implement fast link fault detection.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) (Optional) Enter the address family configuration mode. To configure this function for a specific address family, please configure only one task.

- Enter the IPv4 unicast configuration mode.

  address-family ipv4 [**unicast**]

- Enter the IPv4 VRF configuration mode.

  address-family ipv4 vrf *vrf-name*

- Enter the IPv6 unicast configuration mode.

  address-family ipv6 [**unicast**]

- Enter the IPv6 VRF configuration mode.

  address-family ipv6 vrf *vrf-name*

(5) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(6) Configure BGP FRR.

bgp fast-reroute

The FRR function is disabled by default.

1.8.4 Configuring EBGP Multi-Path Bypass Protection

1. Overview

After EBGP multi-path bypass protection is configured, when all ECMP routes fail, the bypass route becomes the primary route for data forwarding.

BGP FRR supports only 1:1 protection. After the equal-cost multi-path routing (ECMP) function is enabled, FRR becomes unavailable. The multi-path bypass protection enables BGP to support 1:N protection. Users can configure BGP multi-path bypass protection to enable the system to select a backup bypass path even if ECMP is configured. When all ECMP routes fail, the bypass route becomes the primary route for forwarding.

When there are multiple paths to the same network in the routing table of BGP, BGP calculates a route with the highest priority by default. After the BGP multi-path bypass protection function is enabled, BGP selects a preferred backup route even if ECMP routes exist. After the fast link detection mechanism of BFD detects that the master link is faulty, the system switches data to the originally calculated backup link for forwarding. After route convergence is completed, the device switches data to the re-calculated optimal path for data forwarding.

2. Restrictions and Guidelines

You can configure a neighbor BFD session to implement fast link fault detection.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure BGP multi-path bypass protection.

bgp install standby-path

Multi-path bypass protection is disabled by default.

(5) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(6) Create a BFD session for the BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **fall-over bfd**

No BFD session is configured for a BGP neighbor by default.

1.8.5 Configuring BGP GR

1. Overview

This section describes how to configure BGP GR to ensure that data transmission is not interrupted during protocol restart and implement the deployment of highly reliable networks.

2. Restrictions and Guidelines

- To successfully deploy the BGP GR function, you need to configure a neighbor as the GR Helper.
- IGP GR also needs to be configured in an IBGP environment.
- After BGP GR is enabled, you need to reset a BGP neighbor connection to make BGP GR take effect.
- After the GR function is enabled in BGP configuration mode, the GR function will be enabled in all address families.
- You can run the **exit-address-family** command to exit the address family configuration mode of BGP.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(5) Configure BGP GR.

bgp graceful-restart

The GR function is enabled by default.

(6) Configure the BGP GR restart timer.

bgp graceful-restart restart-time *restart-time*

The default timer value is **120** seconds.

(7) (Optional) Configure the BGP GR routing aging timer.

bgp graceful-restart stalepath-time *time*

The default value of the aging timer is **360** seconds.

1.8.6 Configuring BGP NSR

1. Overview

During switchover between master and slave supervisor engines, the NSR function keeps the network topology stable, maintains neighbor status and forwarding table, and ensures that key services are not interrupted.

2. Restrictions and Guidelines

- To deploy the BGP NSR function, rely on the device to support the function of dual engine redundancy.
- After the BGP NSR function is enabled, connections to the BGP neighbors will be reset for the function to take effect.
- The neighbor based NSR command is equivalent to the **bgp nsr** command. This function enables the NSR function for all neighbors.
- You are not advised to use the neighbor-based NSR command as it is to be abandoned.
- When the BGP NSR function is enabled for a neighbor, the connection to the neighbor will be reset and the TCP none-stop-service (NSS) will be enabled for the neighbor. Then, relevant neighbor and routing information will be backed up to the slave supervisor engine. In this case, if the NSR function is enabled after a BGP speaker is in the established state, the neighbor relationship will be re-established, causing neighbor flapping. You are advised to enable NSR before a neighbor relationship is established between peers.
- The NSR function does not take effect on a neighbor that fails to establish a BGP connection. That is, if the BGP connection of a neighbor is not in the established state, the neighbor will not execute the NSR operation. Only a neighbor in the established state will perform NSR-related backup operations.
- Supporting the BGP NSR function does not mean that the device can perform switchovers between the active and standby management boards. To perform such switchovers, you must depend on the device hardware. NSR devices must support the function of dual engine redundancy.
- If the BGP or TCP backup is not complete, the current BGP NSR switchover may fail. When a NSR switchover failure occurs, routes can be still recovered through BGP GR. Therefore, you are advised to enable both BGP NSR and BGP GR.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Create a BGP neighbor.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **remote-as** *as-number*

(5) Configure the BGP NSR function.

bgp nsr

The NSR function is disabled by default.

1.8.7 Configuring BGP Session Retention

1. Overview

For devices that support BGP, routing errors in an address family will affect route stability in other address families: When a device receives an update packet from a neighbor and an error on the multi-protocol routing

attribute is detected, the device will disconnect the BGP session. As a result, flapping occurs on routes in all address families of this neighbor.

After the BGP session retention function is enabled, if an error occurs in the routing attribute of an address family, only the routing information related to the neighbor in this address family is deleted. The BGP session and other address families are not affected, which enhances the stability of BGP.

Recovery-time specifies the waiting time for automatic route recovery. A neighbor must support the route-refresh capability so that the time can be set. After the recovery-time elapses, BGP sends the route-refresh message of the address family to the neighbor and re-advertises all routing information in the address family to this neighbor.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure BGP to retain BGP sessions when it detects a multiprotocol path error.

bgp mp-error-handle session-retain [**refresh-timer** *refresh-timer*]

BGP terminates BGP sessions by default when it detects a multiprotocol route error.

1.9 Enabling the Extended Functions of BGP

1.9.1 Configuration Tasks

The configuration of BGP extended functions includes the following tasks: All configuration tasks are optional and may be selected as needed.

- Configuring BMP Monitoring
- Configuring the Administrative Distance of BGP

1.9.2 Configuring BMP Monitoring

1. Overview

After BMP monitoring is configured, BMP is monitored by the BMP server, which focuses on the status of BGP peers, peer entry transmission and receiving, and all kinds of peer statistics.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a BMP server instance.

bmp server *server-number*

(4) Configure the address and port number of the BMP server.

address [*bmp-server-ipv4-address* | *bmp-server-ipv6-address*] **port** *port-number*

The address and port number of the BMP server are not configured in BMP mode by default.

(5) Configure an outbound interface for establishing a TCP connection with the BMP server.

update-source *interface-type interface-number*

The system automatically selects the outbound interface for a TCP connection based on the IP address of the BMP server by default. The outbound interface of local packets is generally used.

(6) Configure the VRF instance, to which a TCP connection to the BMP server belongs.

vrf *vrf-name*

A TCP connection is established with the BMP server in the default VRF instance by default.

(7) (Optional) Configure the interval for re-establishing a TCP connection with the BMP server.

failure-retry-delay *time*

The interval for reconnecting to the BMP server gradually increases from the initial **30** seconds by default.

(8) (Optional) Configure a description for the BMP server instance.

description *text*

No description is configured for a BMP server instance by default.

(9) Configure the BMP server to monitor routes that are received from peers and have a routing policy applied.

adj-rib-in post-policy

The BMP server does not monitor routes that are received from a BGP peer and have a routing policy applied by default.

(10) Configure the BMP server to monitor routes that are received from a peer and are not renamed.

adj-rib-in pre-policy

The BMP server does not monitor routes that are received from a BGP peer and are not renamed by default.

(11) Configure the BMP server to monitor routes that are sent to a peer and have a routing policy applied.

adj-rib-out post-policy

The BMP server does not monitor routes that are sent to a BGP peer and have a routing policy applied by default.

(12) Configure the BMP server to monitor a BGP peer.

neighbor { *neighbor-ipv4-address* | *neighbor-ipv6-address* | *peer-group-name* } **bmp-active** { **all** | **server** *server-number* [*server-number* [*server-number*]] }

BGP peers are not monitored by the BMP server by default.

(13) Enable the packet mirroring function of BGP.

route mirroring

The BMP server does not send route mirroring packets by default.

(14) Configure the interval for BMP server to send status statistics.

stats-reporting-period *time*

When status statistics of a monitored peer are changed, BMP delays a period of time in sending the status statistics to the BMP server by default.

1.9.3 Configuring the Administrative Distance of BGP

1. Overview

The administrative distance is used to evaluate the reliability of various route sources. A smaller administrative distance indicates a better route.

- Administrative distance of BGP

  The administrative distance indicates the reliability of a route source. The value range is from 1 to 255. A larger administrative distance indicates a lower route reliability. BGP sets different administrative distances for sources, from which routing information is learned. Administrative distances are classified into external-distances, internal-distances, and local-distances.

  - External-distance: Indicates the administrative distances of routes learned from EBGP peers.
  - Internal-distance: Indicates the administrative distances of routes learned from IBGP peers.
  - Local-distance: Indicates the administrative distances of routes learned from peers but it is considered that better routes can be learned from IGP. Generally, these routes can be indicated by the **network backdoor** command.

- Backdoor route

  If you prefer an IGP route without using this EBGP route, you can configure this EBGP route as the backdoor route. The default administrative distance of routes learned from a BGP speaker that has established an EBGP connection is **20**. You can run the **network backdoor** command to set the administrative distance of EBGP routes to 200 so that routes learned from IGP have a higher priority. Routes learned from IGP are considered as backdoor routes and are not advertised externally.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable BGP to enter the BGP configuration mode.

router bgp *as-number*

(4) Configure the administrative distance of a BGP route.

distance bgp *external-distance internal-distance local-distance*

The default administrative distance of a route learned by BGP from an EBGP peer is **20** and that of a route learned by BGP from an IBGP peer is **200**.

(5) Configure a backdoor route.

network *network-number* [**mask** *mask*] [**route-map** *map-tag*] **backdoor**

No backdoor route is configured by default.

1.10 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

Running the **clear** command during operation of the device may lose vital information and interrupt services.

Run the **debug** commands to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging switch immediately after use.

Table 1-2 Monitoring

Command	Purpose
clear ip bgp [**vrf** *vrf-name*] { * | *as-number* | *neighbor-ipv4-address* | *neighbor-ipv6-address* } [**soft**] [**in** | **out**] **clear bgp ipv4 unicast** [**vrf** *vrf-name*] { ***** | *as-number* | *neighbor-ipv4-address* | *neighbor-ipv6-address* } [**soft**] [**in** | **out**] **clear ip bgp** [**vrf** *vrf-name*] **update-group** [*update-group-index* | *neighbor-ipv4-address* | *neighbor-ipv6-address*] [**soft**] [**in** | **out**] **clear bgp ipv4 unicast** [**vrf** *vrf-name*] **update-group** [*update-group-index* | *neighbor-ipv4-address* | *neighbor-ipv6-address*] [**soft**] [**in** | **out**]	Clears BGP IPv4 unicast routes.
clear bgp ipv6 unicast [**vrf** *vrf-name*] { ***** | *as-number* | *neighbor-ipv4-address* | *neighbor-ipv6-address* } [**soft**] [**in** | **out**] **clear bgp ipv6 unicast** [**vrf** *vrf-name*] **update-group** [*update-group-index* | *neighbor-ipv4-address* | *neighbor-ipv6-address*] [**soft**] [**in** | **out**]	Clears BGP IPv6 unicast routes.
clear bgp advertise lowest-priority on-startup	Restores the priority of routes advertised by BGP to a neighbor to the one before the priority is adjusted to the lowest.
show ip bgp **show bgp ipv4 unicast**	Displays BGP IPv4 unicast routes.

Command	Purpose
show ip bgp [**vrf** *vrf-name*] **update-group** [*neighbor-ipv4-address* | *neighbor-ipv6-address* | *update-group-index*] [**summary**] **show bgp ipv4 unicast** [**vrf** *vrf-name*] **update-group** [*neighbor-ipv4-address* | *neighbor-ipv6-address* | *update-group-index*] [**summary**]	Displays the update-group information of the BGP IPv4 unicast address family.
show bgp ipv6 unicast	Displays BGP IPv6 unicast routes.
show bgp ipv6 unicast [**vrf** *vrf-name*] **update-group** [*neighbor-ipv4-address* | *neighbor-ipv6-address* | *update-group-index*] [**summary**]	Displays the update-group information of the BGP IPv6 unicast address family.
show bgp bmp server [*server-number* [**detail**] | **detail**] }	Displays information about a BMP server instance.
show bgp bmp neighbor	Displays information about neighbors monitored by the BMP server.
show bgp bmp summary	Displays the summary of an established connection to the BMP server.
show bgp statistics [**vrf** *vrf-name*]	Displays BGP statistics.
debug ip bgp all	Debugs BGP.
debug ip bgp bmp	Debugs BGP BMP.
debug ip bgp dampening	Debugs route flapping of BGP.
debug ip bgp event	Debugs event processing of BGP.
debug ip bgp filter	Debugs route filtering of BGP.
debug ip bgp fsm	Debugs BGP state machine.
debug ip bgp keepalives	Debugs neighbor keepalive of BGP.
debug ip bgp nsm	Debugs core route processing of BGP.
debug ip bgp update	Debugs BGP update packets.
debug ip bgp update-group	Debugs the update-group function of BGP.
debug ip bgp add-path	Debugs the ADD-PATH function of BGP.

1.11 Configuration Examples

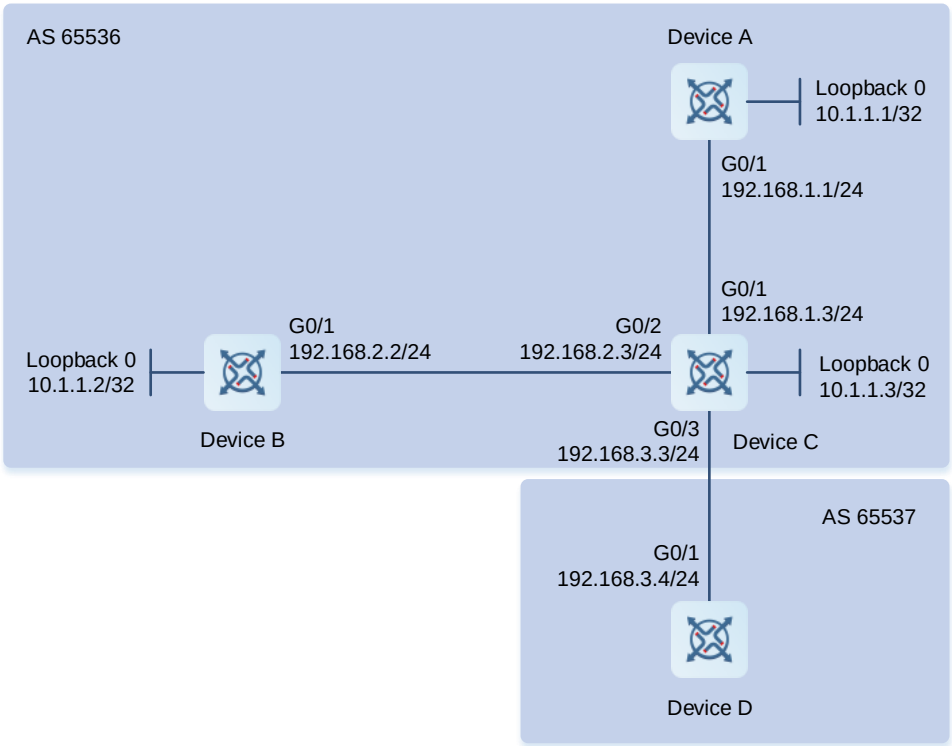
1.11.1 Configuring BGP Basic Networking

1. Requirements

BGP speakers need to establish IBGP neighbor relationships and EBGP neighbor relationships to implement basic networking.

2. Topology

Figure 1-2 Topology of BGP Basic Networking



3. Notes

- Enable BGP on all devices and set AS numbers for the devices as shown in Figure 1-2 (omitted).
- Configure a loopback interface on each of devices A, B, and C, which establish IBGP neighbor relationships through the loopback interfaces.
- Configure devices C and D to establish an EBGP neighbor relationship through directly connected interfaces.
- Create an IBGP peer group on device C.

4. Procedure

(1) Configure loopback interfaces and IP addresses for the interfaces.

Configure device A.

```
Device A# configure terminal
Device A(config)# interface loopback 0
```

```
Device A(config-if-Loopback 0)# ip address 10.1.1.1 255.255.255.255
Device A(config-if-Loopback 0)# exit
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/1)# exit
```

Configure device B.

```
Device B# configure terminal
Device B(config)# interface loopback 0
Device B(config-if-Loopback 0)# ip address 10.1.1.2 255.255.255.255
Device B(config-if-Loopback 0)# exit
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
```

Configure device C.

```
Device C# configure terminal
Device C(config)# interface loopback 0
Device C(config-if-Loopback 0)# ip address 10.1.1.3 255.255.255.255
Device C(config-if-Loopback 0)# exit
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip address 192.168.1.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface GigabitEthernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ip address 192.168.2.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/2)# exit
Device C(config)# interface GigabitEthernet 0/3
Device C(config-if-GigabitEthernet 0/3)# ip address 192.168.3.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/3)# exit
```

Configure device D.

```
Device D# configure terminal
Device D(config)# interface GigabitEthernet 0/1
Device D(config-if-GigabitEthernet 0/1)# ip address 192.168.3.4 255.255.255.0
Device D(config-if-GigabitEthernet 0/1)# exit
```

(2) Enable BGP and configure the loopback interfaces as neighbor interfaces.

Configure device A.

```
Device A(config)# router bgp 65536
Device A(config-router)# neighbor 10.1.1.3 remote-as 65536
Device A(config-router)# neighbor 10.1.1.3 update-source loopback 0
```

Configure device B.

```
Device B(config)# router bgp 65536
Device B(config-router)# neighbor 10.1.1.3 remote-as 65536
Device B(config-router)# neighbor 10.1.1.3 update-source loopback 0
```

Configure device C.

```
Device C(config)# router bgp 65536
```

```
Device C(config-router)# neighbor ibgp-group peer-group
Device C(config-router)# neighbor ibgp-group remote-as 65536
Device C(config-router)# neighbor ibgp-group update-source loopback 0
Device C(config-router)# neighbor 10.1.1.1 peer-group ibgp-group
Device C(config-router)# neighbor 10.1.1.2 peer-group ibgp-group
Device C(config-router)# neighbor 192.168.3.4 remote-as 65537
```

Configure device D.

```
Device D(config)# router bgp 65537
Device D(config-router)# neighbor 192.168.3.3 remote-as 65536
```

5. Verification

On device A, run the **show ip bgp neighbor** command to display the BGP neighbor status.

```
Device A# show ip bgp neighbor
BGP neighbor is 10.1.1.3, remote AS 65536, local AS 65536, internal link
  BGP version 4, remote router ID 10.1.1.3
  BGP state = Established, up for 00:00:05
  Last read        , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:1
    refresh message:0 dynamic cap:0 notifications:0
  Sent 2 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:1
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 0 seconds
  Update source is Loopback 0

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.1.1.1, Local port: 1039
Foreign host: 10.1.1.3, Foreign port: 179
Nexthop: 10.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset:        , due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)
```

On device B, run the **show** command to display the BGP neighbor status.

```
Device B# show ip bgp neighbor
BGP neighbor is 10.1.1.3, remote AS 65536, local AS 65536, internal link
  BGP version 4, remote router ID 10.1.1.3
  BGP state = Established, up for 00:00:07
  Last read        , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:1
    refresh message:0 dynamic cap:0 notifications:0
  Sent 2 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:1
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 0 seconds
  Update source is Loopback 0

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.1.1.2, Local port: 1041
Foreign host: 10.1.1.3, Foreign port: 179
Nexthop: 10.1.1.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset:        , due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)
```

On device C, run the **show** command to display the BGP neighbor status.

```
Device C# show ip bgp neighbor
BGP neighbor is 10.1.1.1, remote AS 65536, local AS 65536, internal link
 Member of peer-group ibgp-group for session parameters
  BGP version 4, remote router ID 10.1.1.1
  BGP state = Established, up for 00:01:13
  Last read        , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
```

```
    Address family IPv4 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:2
    refresh message:0 dynamic cap:0 notifications:0
  Sent 3 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:2
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 0 seconds
  Update source is Loopback 0

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  ibgp-group peer-group member
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.1.1.3, Local port: 179
Foreign host: 10.1.1.1, Foreign port: 1039
Nexthop: 10.1.1.3
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 10.1.1.2, remote AS 65536, local AS 65536, internal link
 Member of peer-group ibgp-group for session parameters
  BGP version 4, remote router ID 10.1.1.2
  BGP state = Established, up for 00:01:17
  Last read        , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:2
    refresh message:0 dynamic cap:0 notifications:0
  Sent 3 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:2
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 0 seconds
  Update source is Loopback 0

 For address family: IPv4 Unicast
```

```
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  ibgp-group peer-group member
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.1.1.3, Local port: 179
Foreign host: 10.1.1.2, Foreign port: 1041
Nexthop: 10.1.1.3
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 192.168.3.4, remote AS 65536, local AS 65536, internal link
 Member of peer-group ibgp-group for session parameters
  BGP version 4, remote router ID 192.168.3.4
  BGP state = Established, up for 00:01:01
  Last read        , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:2
    refresh message:0 dynamic cap:0 notifications:0
  Sent 3 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:2
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 0 seconds
  Update source is Loopback 0

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  ibgp-group peer-group member
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 192.168.3.3, Local port: 179
Foreign host: 192.168.3.4, Foreign port: 1018
Nexthop: 192.168.3.3
Nexthop global: ::
Nexthop local: ::
```

```
BGP connection: non shared network
```

On device D, run the **show** command to display the BGP neighbor status.

```
Device D# show ip bgp neighbor
BGP neighbor is 192.168.3.3, remote AS 65536, local AS 65536, internal link
 Member of peer-group ibgp-group for session parameters
  BGP version 4, remote router ID 10.1.1.3
  BGP state = Established, up for 00:01:01
  Last read        , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:2
    refresh message:0 dynamic cap:0 notifications:0
  Sent 3 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:2
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 0 seconds
  Update source is Loopback 0

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  ibgp-group peer-group member
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 192.168.3.4, Local port: 1018
Foreign host: 192.168.3.3, Foreign port: 179
Nexthop: 192.168.3.4
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.168.1.1 255.255.255.0
!
interface Loopback 0
 ip address 10.1.1.1 255.255.255.255
```

```
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.3 remote-as 65536
 neighbor 10.1.1.3 update-source Loopback 0
 address-family ipv4
  neighbor 10.1.1.3 activate
  exit-address-family
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.168.2.2 255.255.255.0
!
interface Loopback 0
 ip address 10.1.1.2 255.255.255.255
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.3 remote-as 65536
 neighbor 10.1.1.3 update-source Loopback 0
 address-family ipv4
  neighbor 10.1.1.3 activate
  exit-address-family
!
```

- Device C configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.168.1.3 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 192.168.2.3 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip address 192.168.3.3 255.255.255.0
```

```
!
interface Loopback 0
 ip address 10.1.1.3 255.255.255.255
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor ibgp-group peer-group
 neighbor ibgp-group remote-as 65536
 neighbor ibgp-group update-source Loopback 0
 neighbor 10.1.1.1 peer-group ibgp-group
 neighbor 10.1.1.2 peer-group ibgp-group
 neighbor 192.168.3.4 remote-as 65537
 address-family ipv4
  no neighbor ibgp-group activate
  neighbor 192.168.3.4 activate
  exit-address-family
!
```

- Device D configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.168.1.3 255.255.255.0
!
router bgp 65537
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 address-family ipv4
  exit-address-family
!
```

7. Common Errors

- IGP is disabled and the local loopback address and the loopback address of an IBGP neighbor cannot interwork with each other, resulting in the failure to establish a neighbor relationship.
- When EBGP neighbors are not directly connected, **ebgp-multihop** is not configured, causing the failure to establish a TCP connection.

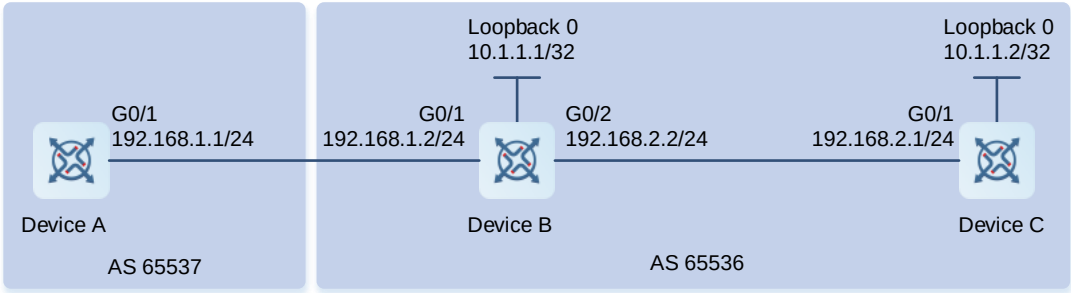
1.11.2 Configuring BGP MD5 Authentication

1. Requirements

The establishment of a TCP connection needs MD5 encryption to ensure data transmission security.

2. Topology

Figure 1-3 Topology of BGP MD5 Authentication



3. Notes

- Enable BGP on all devices and set AS numbers for the devices as shown in Figure 1-3 (omitted).
- Configure a loopback interface on each of devices B and C, which establish an IBGP neighbor relationship through the loopback interfaces (omitted).
- Configure devices A and B to establish an EBGP neighbor relationship through directly connected interfaces.
- On devices A, B, and C, configure passwords for their neighbors.

4. Procedure

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65537
Device A(config-router)# neighbor 192.168.1.2 remote-as 65536
Device A(config-router)# neighbor 192.168.1.2 password 7 ebgpneighbor
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 65536
Device B(config-router)# neighbor 10.1.1.2 remote-as 65536
Device B(config-router)# neighbor 10.1.1.2 update-source loopback 0
Device B(config-router)# neighbor 10.1.1.2 password ibgpneighbor
Device B(config-router)# neighbor 192.168.1.1 remote-as 65537
Device B(config-router)# neighbor 192.168.1.1 password 7 ebgpneighbor
```

Configure device C.

```
Device C# configure terminal
Device C(config)# router bgp 65536
Device C(config-router)# neighbor 10.1.1.1 remote-as 65536
Device C(config-router)# neighbor 10.1.1.1 update-source loopback 0
Device C(config-router)# neighbor 10.1.1.1 password ibgpneighbor
```

5. Verification

On device A, run the **show ip bgp neighbors** command to display the BGP neighbor status.

```
Device A# show ip bgp neighbors
BGP neighbor is 192.168.1.2, remote AS 65536, local AS 65537, external link
  BGP version 4, remote router ID 10.1.1.1
  BGP state = Established, up for 00:04:54
  Last read        , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 7 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:6
    refresh message:0 dynamic cap:0 notifications:0
  Sent 7 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:6
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 192.168.1.1, Local port: 1026
Foreign host: 192.168.1.2, Foreign port: 179
Nexthop: 192.168.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:04:54, due to BGP Notification sent
Notification Error Message: (Cease/Administratively Reset.)
```

On device B, run the **show ip bgp neighbors** command to display the BGP neighbor status.

```
Device B# show ip bgp neighbors
BGP neighbor is 10.1.1.2, remote AS 65536, local AS 65536, internal link
  BGP version 4, remote router ID 10.1.1.2
  BGP state = Established, up for 00:04:01
  Last read        , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 8 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:7
    refresh message:0 dynamic cap:0 notifications:0
```

```
  Sent 8 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:7
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 10.1.1.1, Local port: 179
Foreign host: 10.1.1.2, Foreign port: 1038
Nexthop: 10.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:05:27, due to BGP Notification received
Notification Error Message: (Cease/Administratively Reset.)

BGP neighbor is 192.168.1.1, remote AS 65537, local AS 65536, external link
  BGP version 4, remote router ID 192.168.1.1
  BGP state = Established, up for 00:05:27
  Last read        , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 8 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:7
    refresh message:0 dynamic cap:0 notifications:0
  Sent 8 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:7
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
```

```
Local host: 192.168.1.2, Local port: 179
Foreign host: 192.168.1.1, Foreign port: 1026
Nexthop: 192.168.1.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:05:27, due to BGP Notification received
Notification Error Message: (Cease/Administratively Reset.)
```

On device C, run the **show ip bgp neighbors** command to display the BGP neighbor status.

```
Device C# show ip bgp neighbors
BGP neighbor is 10.1.1.1, remote AS 65536, local AS 65536, internal link
  BGP version 4, remote router ID 10.1.1.1
  BGP state = Established, up for 00:04:01
  Last read        , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 8 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:7
    refresh message:0 dynamic cap:0 notifications:0
  Sent 8 messages, 0 notifications, 0 in queue
    open message:1 update message:0 keepalive message:7
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 10.1.1.2, Local port: 1038
Foreign host: 10.1.1.1, Foreign port: 179
Nexthop: 10.1.1.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:05:27, due to BGP Notification received
Notification Error Message: (Cease/Administratively Reset.)
```

6. Configuration Files

- Device A configuration file

```
!
```

```
router bgp 65537
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.1.2 password 7 ebgpneighbor
 address-family ipv4
  neighbor 192.168.1.2 activate
  exit-address-family
!
```

- Device B configuration file

```
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.2 remote-as 65536
 neighbor 10.1.1.2 update-source Loopback 0
 neighbor 10.1.1.2 password ibgpneighbor
 neighbor 192.168.1.1 remote-as 65537
 neighbor 192.168.1.1 password 7 ebgpneighbor
 address-family ipv4
  neighbor 10.1.1.2 activate
  neighbor 192.168.1.1 activate
  exit-address-family
!
```

- Device C configuration file

```
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.1 remote-as 65536
 neighbor 10.1.1.1 update-source Loopback 0
 neighbor 10.1.1.1 password ibgpneighbor
 address-family ipv4
  neighbor 10.1.1.1 activate
  exit-address-family
!
```

7. Common Errors

- The passwords for MD5 authentication are different on both sides of a BGP neighbor relationship.

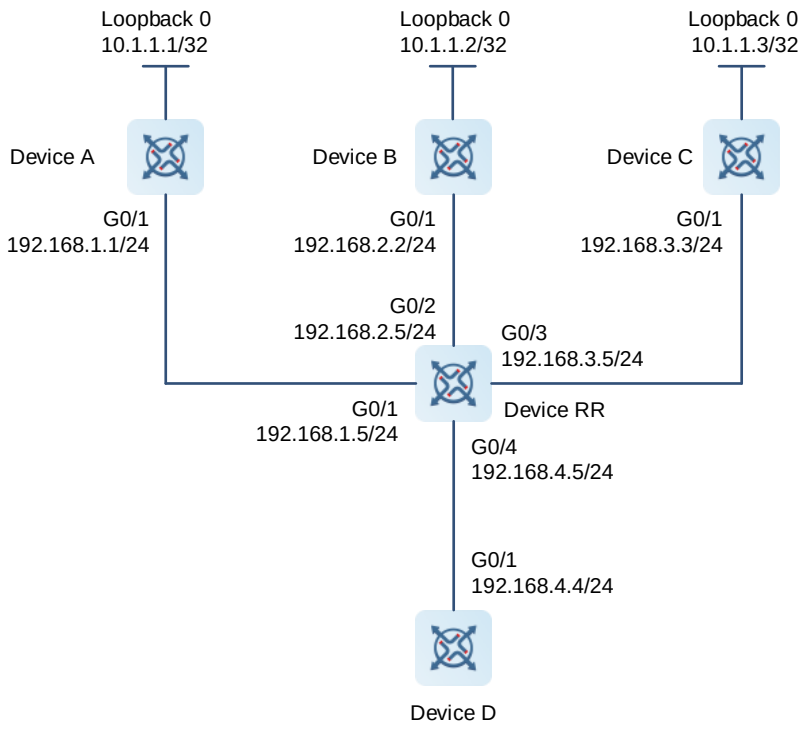
1.11.3 Configuring a BGP Route Reflector

1. Requirements

In a network involving many BGP speakers, a route reflector needs to be configured to simplify the management and synchronization of routing information and make routing more efficient.

2. Topology

Figure 1-4 Topology of BGP Route Reflector



3. Notes

- Enable BGP on all devices and set AS numbers for the devices as shown in Figure 1-4 (omitted).
- Configure a loopback interface on each device and configure the devices to establish IBGP neighbor relationships through the loopback interfaces according to connection lines shown in the figure above (omitted).
- Configure route reflection on device RR and specify devices A, B, C, and D as reflection clients.

4. Procedure

(1) Configure BGP neighbors to advertise network information.

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65536
Device A(config-router)# neighbor 10.1.1.5 remote-as 65536
Device A(config-router)# neighbor 10.1.1.5 update-source loopback 0
Device A(config-router)# network 192.168.1.0 mask 255.255.255.0
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 65536
Device B(config-router)# neighbor 10.1.1.5 remote-as 65536
Device B(config-router)# neighbor 10.1.1.5 update-source loopback 0
```

Configure device C.

```
Device C# configure terminal
Device C(config)# router bgp 65536
Device C(config-router)# neighbor 10.1.1.5 remote-as 65536
Device C(config-router)# neighbor 10.1.1.5 update-source loopback 0
```

Configure device D.

```
Device D# configure terminal
Device D(config)# router bgp 65536
Device D(config-router)# neighbor 10.1.1.5 remote-as 65536
Device D(config-router)# neighbor 10.1.1.5 update-source loopback 0
```

(2) Configure a route reflector.

Configure device RR.

```
Device RR# configure terminal
Device RR(config)# router bgp 65536
Device RR(config-router)# neighbor 10.1.1.1 remote-as 65536
Device RR(config-router)# neighbor 10.1.1.1 update-source loopback 0
Device RR(config-router)# neighbor 10.1.1.1 route-reflector-client
Device RR(config-router)# neighbor 10.1.1.2 remote-as 65536
Device RR(config-router)# neighbor 10.1.1.2 update-source loopback 0
Device RR(config-router)# neighbor 10.1.1.2 route-reflector-client
Device RR(config-router)# neighbor 10.1.1.3 remote-as 65536
Device RR(config-router)# neighbor 10.1.1.3 update-source loopback 0
Device RR(config-router)# neighbor 10.1.1.3 route-reflector-client
Device RR(config-router)# neighbor 10.1.1.4 remote-as 65536
Device RR(config-router)# neighbor 10.1.1.4 update-source loopback 0
Device RR(config-router)# neighbor 10.1.1.4 route-reflector-client
```

5. Verification

On device RR, check the BGP neighbor status.

```
Device RR# show ip bgp summary
BGP router identifier 10.1.1.5, local AS number 65536
BGP table version is 1
0 BGP AS-PATH entries
0 BGP Community entries
1 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor       V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.1.1.1       4      65536      8      9       1    0    0 00:05:11       1
10.1.1.2       4      65536      9      9       1    0    0 00:05:24       0
```

```
10.1.1.3       4      65536      8      7       1    0    0 00:05:10       0
10.1.1.4       4      65536      9      8       1    0    0 00:05:14       0

Device RR# show ip bgp
BGP table version is 1, local router ID is 10.1.1.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf     Weight Path
*>i192.168.1.0     10.1.1.1                 0        100          0    i

Total number of prefixes 1
```

On device D, run the **show ip bgp summary** command to display BGP details.

```
Device D# show ip bgp summary
BGP router identifier 10.1.1.4, local AS number 65536
BGP table version is 1
0 BGP AS-PATH entries
0 BGP Community entries
1 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor       V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.1.1.5       4      65536      8      9       1    0    0 00:05:20       1

Device D# show ip bgp
BGP table version is 1, local router ID is 10.1.1.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf     Weight Path
* i192.168.1.0     10.1.1.1                 0        100          0    i

Total number of prefixes 1
```

6. Configuration Files

- Device A configuration file

```
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.5 remote-as 65536
```

```
 neighbor 10.1.1.5 update-source Loopback 0
 address-family ipv4
  network 192.168.1.0
  neighbor 10.1.1.5 activate
  exit-address-family
!
```

- Device B configuration file

```
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.5 remote-as 65536
 neighbor 10.1.1.5 update-source Loopback 0
 address-family ipv4
  neighbor 10.1.1.5 activate
  exit-address-family
!
```

- Device C configuration file

```
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.5 remote-as 65536
 neighbor 10.1.1.5 update-source Loopback 0
 address-family ipv4
  neighbor 10.1.1.5 activate
  exit-address-family
!
```

- Device D configuration file

```
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.5 remote-as 65536
 neighbor 10.1.1.5 update-source Loopback 0
 address-family ipv4
  neighbor 10.1.1.5 activate
  exit-address-family
!
```

- Device RR configuration file

```
!
router bgp 65536
 bgp confederation identifier 100
 bgp confederation peers 65537
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.1 remote-as 65536
 neighbor 10.1.1.1 update-source Loopback 0
 neighbor 10.1.1.2 remote-as 65536
 neighbor 10.1.1.2 update-source Loopback 0
 neighbor 10.1.1.3 remote-as 65536
 neighbor 10.1.1.3 update-source Loopback 0
 neighbor 10.1.1.4 remote-as 65536
 neighbor 10.1.1.4 update-source Loopback 0
 address-family ipv4
  network 192.168.1.0
  neighbor 10.1.1.1 activate
  neighbor 10.1.1.1 route-reflector-client
  neighbor 10.1.1.2 activate
  neighbor 10.1.1.2 route-reflector-client
  neighbor 10.1.1.3 activate
  neighbor 10.1.1.3 route-reflector-client
  neighbor 10.1.1.4 activate
  neighbor 10.1.1.4 route-reflector-client
  exit-address-family
!
```

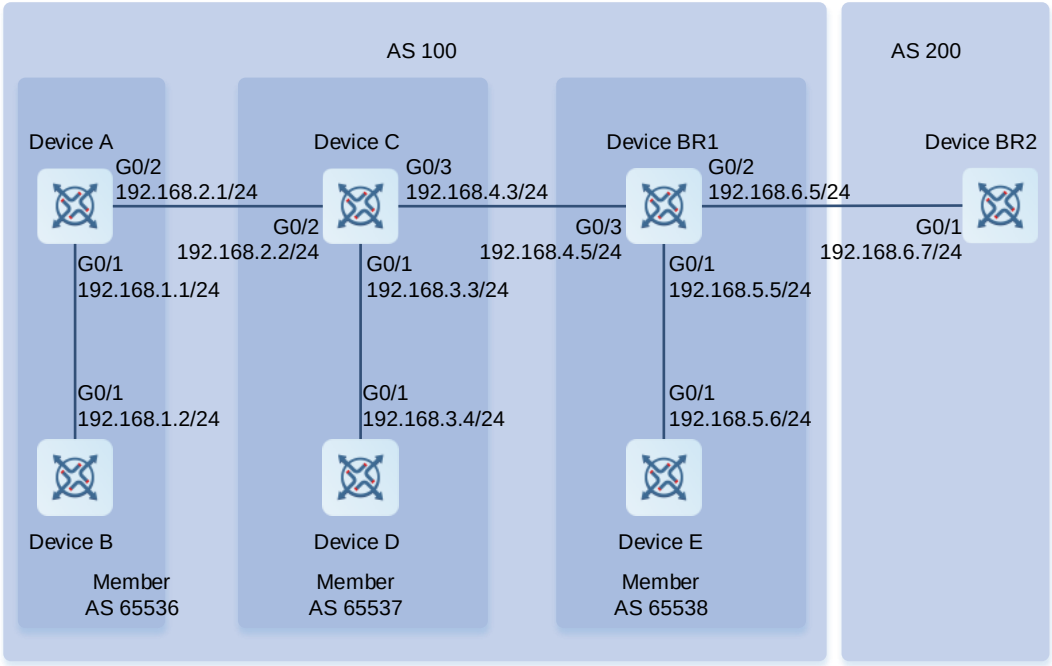
1.11.4 Configuring a BGP Alliance

1. Requirements

A BGP alliance needs to be configured to solve the problem of too many maintenance resources due to excessive IBGP connections in the network.

2. Topology

Figure 1-5 Topology of BGP Alliance



3. Notes

- Configure IP addresses for device interfaces (omitted).
- On devices A and B, configure BGP, set the member AS number to **65536**, and configure an IBGP neighbor relationship.
- On devices C and D, configure BGP, set the member AS number to **65537**, and configure an IBGP neighbor relationship.
- On devices BR1 and E, configure BGP, set the member AS number to **65538**, and configure an IBGP neighbor relationship.
- On devices A, B, C, D, E, and BR1, set the alliance ID to **100**.
- On device A, configure 65537 as the alliance number, configure device C as an EBGP neighbor, and set the peer AS number to **65537**.
- On device C, set the alliance member numbers to **65536** and **65538**, configure device A as an EBGP neighbor and set the peer AS number to **65536**, configure device BR1 as an EBGP neighbor and set the peer AS number to **65538**.
- On device BR1, set the alliance member number to **65537**, configure device C as an EBGP neighbor and set the peer AS number to **65537**, configure device BR2 as an EBGP neighbor and set the peer AS number to **200**.
- On device BR2, configure BGP, set the AS number to **200**, configure device BR1 an EBGP neighbor, and set the peer AS number to **100**.

4. Procedure

(1) Configure IBGP neighbors and EBGP neighbors to advertise network information.

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65536
Device A(config-router)# neighbor 10.1.1.2 remote-as 65536
Device A(config-router)# neighbor 10.1.1.2 update-source loopback 0
Device A(config-router)# neighbor 10.1.1.3 remote-as 65537
Device A(config-router)# neighbor 10.1.1.3 ebgp-multihop 2
Device A(config-router)# neighbor 10.1.1.3 update-source loopback 0
Device A(config-router)# network 192.168.1.0 mask 255.255.255.0
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 65536
Device B(config-router)# neighbor 10.1.1.1 remote-as 65536
Device B(config-router)# neighbor 10.1.1.1 update-source loopback 0
```

Configure device C.

```
Device C# configure terminal
Device C(config)# router bgp 65537
Device C(config-router)# neighbor 10.1.1.1 remote-as 65536
Device C(config-router)# neighbor 10.1.1.1 update-source loopback 0
Device C(config-router)# neighbor 10.1.1.1 ebgp-multihop 2
Device C(config-router)# neighbor 10.1.1.4 remote-as 65537
Device C(config-router)# neighbor 10.1.1.4 update-source loopback 0
Device C(config-router)# neighbor 10.1.1.5 remote-as 65538
Device C(config-router)# neighbor 10.1.1.5 update-source loopback 0
Device C(config-router)# neighbor 10.1.1.5 ebgp-multihop 2
```

Configure device D.

```
Device D# configure terminal
Device D(config)# router bgp 65537
Device D(config-router)# neighbor 10.1.1.3 remote-as 65537
Device D(config-router)# neighbor 10.1.1.3 update-source loopback 0
```

Configure device E.

```
Device E# configure terminal
Device E(config)# router bgp 65538
Device E(config-router)# neighbor 10.1.1.5 remote-as 65538
Device E(config-router)# neighbor 10.1.1.5 update-source loopback 0
```

Configure device BR1.

```
Device BR1# configure terminal
Device BR1(config)# router bgp 65538
Device BR1(config-router)# neighbor 10.1.1.3 remote-as 65537
Device BR1(config-router)# neighbor 10.1.1.3 update-source loopback 0
Device BR1(config-router)# neighbor 10.1.1.3 ebgp-multihop 2
Device BR1(config-router)# neighbor 10.1.1.6 remote-as 65538
Device BR1(config-router)# neighbor 10.1.1.6 update-source loopback 0
```

```
Device BR1(config-router)# neighbor 192.168.6.7 remote-as 200
```

Configure device BR2.

```
Device BR2# configure terminal
Device BR2(config)# router bgp 200
Device BR2(config-router)# neighbor 192.168.6.5 remote-as 100
Device BR2(config-router)# network 192.168.6.0 mask 255.255.255.0
```

(2) Configuring alliance members.

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65536
Device A(config-router)# bgp confederation identifier 100
Device A(config-router)# bgp confederation peers 65537
```

Configure device C.

```
Device C# configure terminal
Device C(config)# router bgp 65537
Device C(config-router)# bgp confederation identifier 100
Device C(config-router)# bgp confederation peers 65536 65538
```

Configure device BR1.

```
Device BR1# configure terminal
Device BR1(config)# router bgp 65538
Device BR1(config-router)# bgp confederation identifier 100
Device BR1(config-router)# bgp confederation peers 65537
```

5. Verification

On device A, check BGP information.

```
Device A# show ip bgp summary
BGP router identifier 10.1.1.1, local AS number 65536
BGP table version is 1
1 BGP AS-PATH entries
0 BGP Community entries
1 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor       V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.1.1.2       4      65536      3      3       1    0    0 00:00:05       0
10.1.1.3       4      65537      3      3       1    0    0 00:00:06       1

Total number of neighbors 1

Device A# show ip bgp
BGP table version is 1, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network          Next Hop            Metric     LocPrf     Weight Path
*  192.168.6.0      192.168.6.7            0        100          0 (65537 65538)
200 i

Total number of prefixes 1
```

On device BR1, check BGP information.

```
Device BR1# show ip bgp summary
BGP router identifier 10.1.1.5, local AS number 200
BGP table version is 2
2 BGP AS-PATH entries
0 BGP Community entries
2 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.1.1.3        4      65537      3      3       2    0    0 00:00:10       1
10.1.1.6        4      65538      3      3       2    0    0 00:00:08       0
192.168.6.7     4        200      3      3       2    0    0 00:00:05       1

Total number of neighbors 1

Device BR1# show ip bgp
BGP table version is 1, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf     Weight Path
*  192.168.1.0      10.1.1.1               0        100          0 (65537 65536) i
*> 192.168.6.0      192.168.6.7            0        100          0 200 i

Total number of prefixes 1
```

On device BR2, check BGP information.

```
Device BR2# show ip bgp summary
BGP router identifier 192.168.6.7, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP Community entries
1 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
192.168.6.5     4        100      3      3       1    0    0 00:00:05       1
```

```
Total number of neighbors 1

Device BR2# show ip bgp
BGP table version is 1, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric     LocPrf     Weight Path
*> 192.168.1.0      192.168.6.5            0        100          0 (65537 65538)
200 i

Total number of prefixes 1
```

6. Configuration Files

- Device A configuration file

```
!
router bgp 65536
 bgp confederation identifier 100
 bgp confederation peers 65537
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.2 remote-as 65536
 neighbor 10.1.1.2 update-source Loopback 0
 neighbor 10.1.1.3 remote-as 65537
 neighbor 10.1.1.3 ebgp-multihop 2
 neighbor 10.1.1.3 update-source Loopback 0
 address-family ipv4
  network 192.168.1.0
  neighbor 10.1.1.2 activate
  neighbor 10.1.1.3 activate
  exit-address-family
!
```

- Device B configuration file

```
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.1 remote-as 65536
 neighbor 10.1.1.1 update-source Loopback 0
 address-family ipv4
  neighbor 10.1.1.1 activate
```

```
  exit-address-family
!
```

- Device C configuration file

```
!
router bgp 65537
 bgp confederation identifier 100
 bgp confederation peers 65536 65538
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.1 remote-as 65536
 neighbor 10.1.1.1 ebgp-multihop 2
 neighbor 10.1.1.1 update-source Loopback 0
 neighbor 10.1.1.4 remote-as 65537
 neighbor 10.1.1.4 update-source Loopback 0
 neighbor 10.1.1.5 remote-as 65538
 neighbor 10.1.1.5 ebgp-multihop 2
 neighbor 10.1.1.5 update-source Loopback 0
 address-family ipv4
  neighbor 10.1.1.1 activate
  neighbor 10.1.1.4 activate
  neighbor 10.1.1.5 activate
  exit-address-family
!
```

- Device D configuration file

```
!
router bgp 65537
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.3 remote-as 65537
 neighbor 10.1.1.3 update-source Loopback 0
 address-family ipv4
  neighbor 10.1.1.3 activate
  exit-address-family
!
```

- Device E configuration file

```
!
router bgp 65538
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
```

```
 neighbor 10.1.1.5 remote-as 65538
 neighbor 10.1.1.5 update-source Loopback 0
 address-family ipv4
  neighbor 10.1.1.5 activate
  exit-address-family
!
```

- Device BR1 configuration file

```
!
router bgp 65538
 bgp confederation identifier 100
 bgp confederation peers 65537
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.3 remote-as 65537
 neighbor 10.1.1.3 ebgp-multihop 2
 neighbor 10.1.1.3 update-source Loopback 0
 neighbor 10.1.1.6 remote-as 65538
 neighbor 10.1.1.6 update-source Loopback 0
 neighbor 192.168.6.7 remote-as 200
 address-family ipv4
  neighbor 10.1.1.3 activate
  neighbor 10.1.1.6 activate
  neighbor 192.168.6.7 activate
  exit-address-family
!
```

- Device BR2 configuration file

```
!
router bgp 200
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.6.5 remote-as 100
 address-family ipv4
  network 192.168.6.0
  neighbor 192.168.6.5 activate
  exit-address-family
!
```

7. Common Errors

- No BGP alliance neighbor is configured.
- A full mesh of connections is not deployed within member ASs of an alliance.

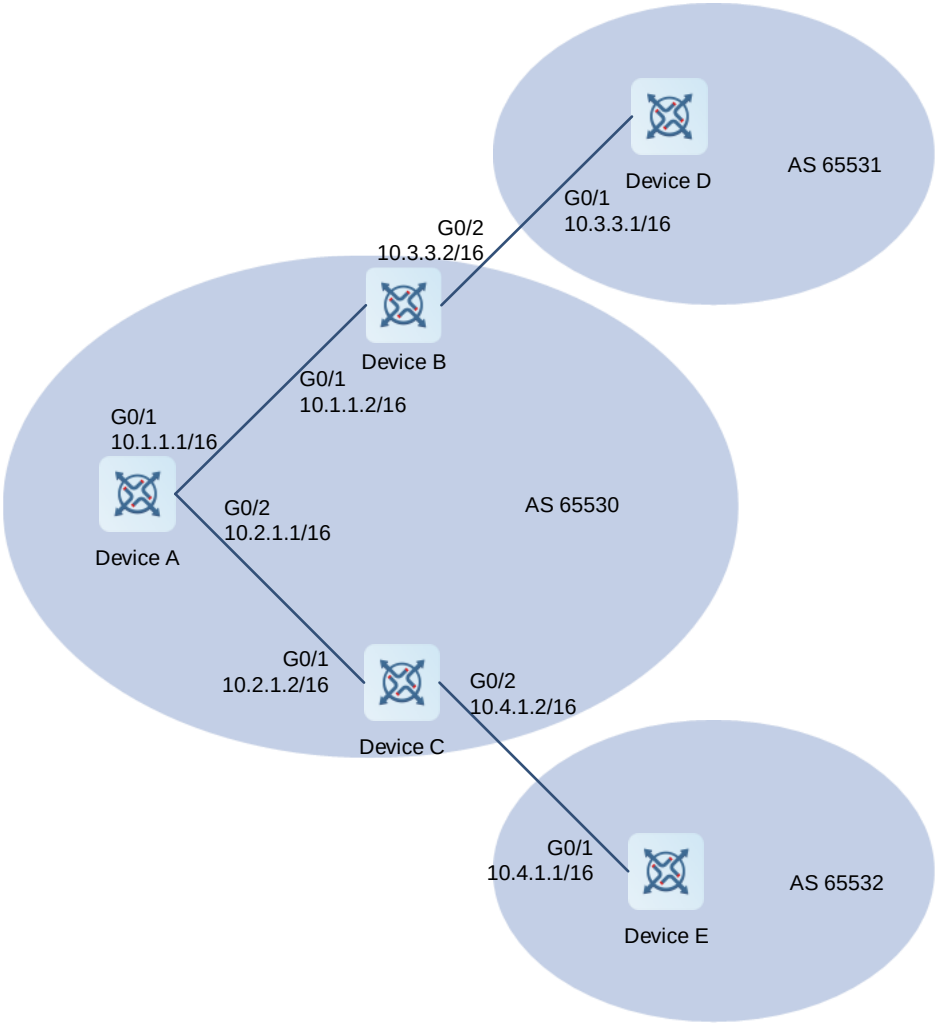
1.11.5 Configuring IBGP Multi-Path Load Balancing

1. Requirements

When there are two routes to the same destination network segment, load balancing needs to be configured to fully utilize network bandwidth resources.

2. Topology

Figure 1-6 Topology of IBGP Multi-Path Load Balancing



3. Notes

- Enable BGP on all devices and set AS numbers for the devices as shown in Figure 1-6 (omitted).
- Configure devices A and B and devices A and C to establish IBGP neighbor relationships through directly connected interfaces (omitted).
- Configure devices B and D and devices C and E to establish EBGP neighbor relationships through directly connected interfaces (omitted).
- Import the same routes to devices D and E.
- On device A, configure IBGP load balancing and enable the AS-PATH loose comparison mode.

4. Procedure

(1) Configure routing information on device A, and re-advertise directly connected route information on devices D and E.

Configure device A.

```
Device A# configure terminal
Device A(config)# ip route 10.3.0.0 255.255.0.0 10.1.1.2
Device A(config)# ip route 10.4.0.0 255.255.0.0 10.2.1.2
```

Configure device D.

```
Device D# configure terminal
Device D(config)# router bgp 65531
Device D(config-router)# redistribute connected
```

Configure device E.

```
Device E# configure terminal
Device E(config)# router bgp 65532
Device E(config-router)# redistribute connected
```

(2) On device A, configure load balancing in AS-PATH loose comparison mode.

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65530
Device A(config-router)# maximum-paths ibgp 2
Device A(config-router)# bgp bestpath as-path multipath-relax
```

5. Verification

On device A, check BGP information.

```
Device A# show ip bgp summary
BGP router identifier 10.2.1.1, local AS number 65530
BGP table version is 9
2 BGP AS-PATH entries
0 BGP Community entries
3 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor       V   AS     MsgRcvd   MsgSent   TblVer   InQ   OutQ   Up/Down
State/PfxRcd
172.16.23.140   4   65530   29       25       8       0     0     00:18:48   2
172.16.23.141   4   65530   24       21       8       0     0     00:17:58   2

Device A# show ip bgp
BGP table version is 9, local router ID is 10.2.1.1
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
*>i10.3.0.0/16     10.3.1.1               0        100          0 65531 ?
```

```
*>i10.4.0.0/16     10.4.1.1              0        100          0 65532 ?
* i10.5.0.0/16     10.3.1.1              0        100          0 65531 ?
*>i              10.4.1.1              0        100          0 65532 ?

Total number of prefixes 3
Device A# show ip bgp 10.5.0.0
BGP routing table entry for 10.5.0.0/16
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  65532
    10.4.1.1 from 10.2.1.2 (172.16.24.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, multipath, best
      Last update: Mon Mar 21 03:45:14 2011

  65531
    10.3.1.1 from 10.1.1.2 (172.16.25.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, multipath
      Last update: Mon Mar 21 03:45:14 2011

Device A# show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.1.0.0/16 is directly connected, FastEthernet 0/0
C    10.1.1.1/32 is local host.
C    10.2.0.0/16 is directly connected, FastEthernet 0/1
C    10.2.1.1/32 is local host.
S    10.3.0.0/16 [1/0] via 10.1.1.2
S    10.4.0.0/16 [1/0] via 10.2.1.2
B    10.5.0.0/16 [200/0] via 10.3.1.1, 00:27:56
                [200/0] via 10.4.1.1, 00:27:56
```

6. Configuration Files

- Device A configuration file

```
!
router bgp 65530
 bgp bestpath as-path multipath-relax
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
```

```
 bgp graceful-restart
 address-family ipv4
  maximum-paths ibgp 2
  exit-address-family
!
ip route 10.3.0.0 255.255.0.0 10.1.1.2
ip route 10.4.0.0 255.255.0.0 10.2.1.2
!
```

- Device D configuration file

```
!
router bgp 65531
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 address-family ipv4
  redistribute connected
  exit-address-family
!
```

- Device E configuration file

```
!
router bgp 65532
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 address-family ipv4
  redistribute connected
  exit-address-family
!
```

7. Common Errors

The priorities of multi-hop BGP paths are different, which causes a load balancing failure.

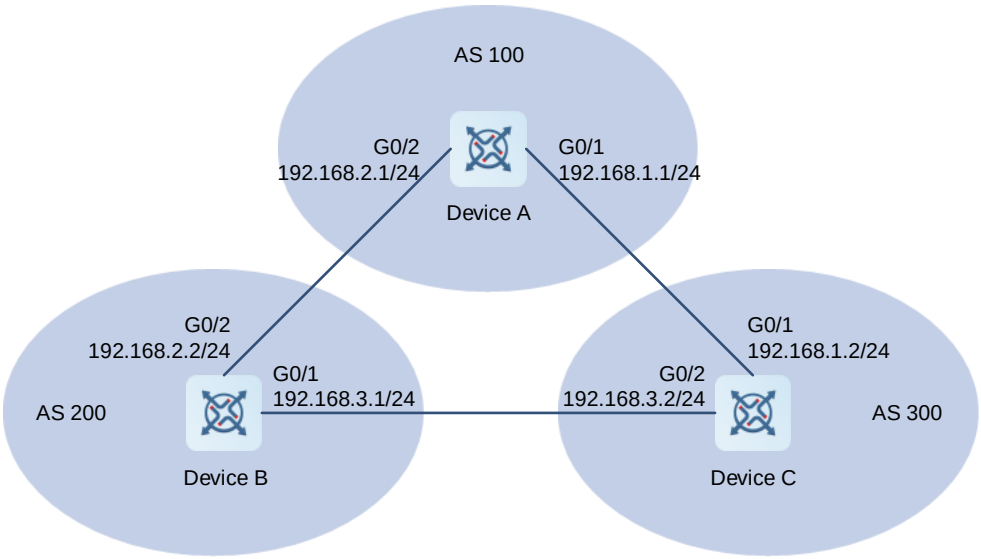
1.11.6 Configuring EBGP FRR

1. Requirements

The FRR function needs to be configured to back up and forward routing information and reduce the delay in service switching.

2. Topology

Figure 1-7 Topology of EBGP FRR



3. Notes

- Enable BGP on all devices (omitted).
- Configure addresses for directly connected interfaces on devices A, B, and C, and configure them to establish EBGP neighbor relationships (omitted).
- Configure a BFD session for the EBGP neighbor relationship between devices B and C.
- Configure FRR on device C.

4. Procedure

(1) Configure interface addresses and interface BFD parameters on devices B and C.

Configure device B.

```
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.3.1 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier
5
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ip address 192.168.2.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/2)# exit
```

Configure device C.

```
Device C# configure terminal
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface GigabitEthernet 0/2
```

```
Device C(config-if-GigabitEthernet 0/2)# ip address 192.168.3.2 255.255.255.0
Device C(config-if-GigabitEthernet 0/2)# bfd interval 200 min_rx 200 multiplier
5
Device C(config-if-GigabitEthernet 0/2)# exit
```

(2) Configure BFD for BGP and BGP FRR.

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 200
Device B(config-router)# neighbor 192.168.3.2 remote-as 300
Device B(config-router)# neighbor 192.168.3.2 fall-over bfd
Device B(config-router)# neighbor 192.168.2.1 remote-as 100
Device B(config-router)# redistribute connect
```

Configure device C.

```
Device C# configure terminal
Device C(config)# router bgp 300
Device C(config-router)# neighbor 192.168.1.1 remote-as 100
Device C(config-router)# neighbor 192.168.3.1 remote-as 200
Device C(config-router)# neighbor 192.168.3.1 fall-over bfd
Device C(config-router)# address-family ipv4 unicast
Device C(config-router-af)# bgp fast-reroute
Device C(config-router-af)# redistribute connect
```

5. Verification

On device C, check BGP information.

```
Device C# show ip bgp summary
BGP router identifier 10.10.10.10, local AS number 300
BGP table version is 12
4 BGP AS-PATH entries
0 BGP Community entries
3 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor       V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
192.168.1.1    4        100     76     77      12   12    0 00:59:27       3
192.168.3.1    4        200     30     30      12   12    0 00:19:03       3

Total number of neighbors 2

Device C# show ip bgp
BGP table version is 12, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric     LocPrf     Weight Path
```

```
*  192.168.1.0     192.168.3.1           0                    0 200 ?
*                192.168.1.1           0                    0 100 ?
*>               0.0.0.0               0                32768    ?
*> 192.168.2.0     192.168.3.1           0                    0 200 ?
*b               192.168.1.1           0                    0 100 ?
*  192.168.3.0     192.168.3.1           0                    0 200 ?
*                192.168.1.1           0                    0 100 200 ?
*>               0.0.0.0               0                32768    ?

Total number of prefixes 3
Device C# show ip bgp 192.168.2.0
BGP routing table entry for 192.168.2.0/24
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  192.168.1.1
  200
    192.168.3.1 from 192.168.3.1 (3.3.3.3)
      Origin incomplete, metric 0, localpref 100, valid, external, best
      Last update: Tue Oct  5 00:26:52 1971

  100
    192.168.1.1 from 192.168.1.1 (44.44.44.44)
      Origin incomplete, metric 0, localpref 100, valid, external, backup
      Last update: Mon Oct  4 23:46:28 1971
Device C# show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, GigabitEthernet 1/9
C    192.168.1.2/32 is local host.
B    192.168.2.0/24 [20/0] via 192.168.3.1, 00:21:39
C    192.168.3.0/24 is directly connected, GigabitEthernet 1/11
C    192.168.3.2/32 is local host.
```

6. Configuration Files

- Device B configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.168.3.1 255.255.255.0
```

```
 bfd interval 200 min_rx 200 multiplier 5
!
interface GigabitEthernet 0/2
 no switchport
 ip address 192.168.2.2 255.255.255.0
!
router bgp 200
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.2.1 remote-as 100
 neighbor 192.168.3.2 remote-as 300
 neighbor 192.168.3.2 fall-over bfd
 address-family ipv4
  redistribute connected
  neighbor 192.168.2.1 activate
  neighbor 192.168.3.2 activate
  exit-address-family
!
```

- Device C configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.168.1.2 255.255.255.0
 bfd interval 200 min_rx 200 multiplier 5
!
interface GigabitEthernet 0/2
 no switchport
 ip address 192.168.3.2 255.255.255.0
 bfd interval 200 min_rx 200 multiplier 5
!
router bgp 300
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.1.1 remote-as 100
 neighbor 192.168.3.1 remote-as 200
 neighbor 192.168.3.1 fall-over bfd
 address-family ipv4
  bgp fast-reroute
  redistribute connected
  neighbor 192.168.1.1 activate
  neighbor 192.168.3.1 activate
  exit-address-family
```

```
!
```

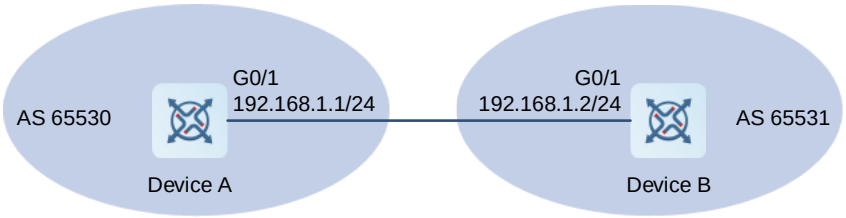
1.11.7 Configuring BGP to Rapidly Withdraw Specified Routes

1. Requirements

Specified routing information needs to be withdrawn.

2. Topology

Figure 1-8 Topology of Fast Withdrawal of Specified Routes



3. Notes

- Enable BGP on all devices (omitted).
- Configure devices A and B to establish a BGP neighbor relationship (omitted).
- Configure an ACL on device A.
- Configure fast withdrawal of specified routes on device A.

4. Procedure

(1) Configure an ACL to permit the address 1.1.1.1.

Configure device A.

```
Device A# configure terminal
Device A(config)# ip access-list standard 1
Device A(config-std-nacl)# permit 1.1.1.1 0.0.0.0
Device A(config-std-nacl)# exit
```

(2) Configure fast withdrawal of the specified route 1.1.1.1.

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65530
Device A(config-router)# neighbor 192.168.1.2 remote-as 65531
Device A(config-router)# bgp fast-withdraw access-list 1
```

5. Verification

On device A, check BGP routing information.

```
Device A# show run router bgp
router bgp 65530
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
```

```
 neighbor 192.168.1.2 remote-as 65531

 address-family ipv4
  bgp fast-withdraw access-list 1
  neighbor 192.168.1.2 activate
 exit-address-family
```

6. Configuration Files

- Device A configuration file

```
!
ip access-list standard 1
 10 permit host 1.1.1.1
!
router bgp 65530
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.1.2 remote-as 65531
 address-family ipv4
  bgp fast-withdraw access-list 1
  neighbor 192.168.1.2 activate
  exit-address-family
!
```

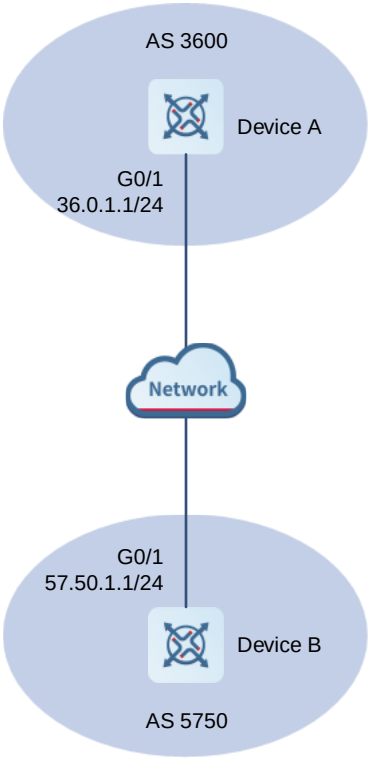
1.11.8 Configuring the BGP Local AS

1. Requirements

When the real AS of the local BGP changes, a new virtual AS 23 can be configured between peers so that the BGP configurations on peers do not need to be configured.

2. Topology

Figure 1-9 Topology of BGP Local AS



3. Notes

- Establish an EBGP neighbor relationship between devices A and B and set the local AS number of the EBGP neighbor to 23.
- Establish an EBGP neighbor relationship with devices A on B.

4. Procedure

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 3600
Device A(config-router)# neighbor 57.50.1.1 remote-as 5750
Device A(config-router)# neighbor 57.50.1.1 update-source loopback 0
Device A(config-router)# neighbor 57.50.1.1 ebgp-multihop 255
Device A(config-router)# neighbor 57.50.1.1 local-as 23 no-prepend replace-as
dual-as
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 5750
Device B(config-router)# neighbor 36.0.1.1 remote-as 23
Device B(config-router)# neighbor 36.0.1.1 update-source loopback 0
Device B(config-router)# neighbor 36.0.1.1 ebgp-multihop 255
```

5. Verification

On device A, check the BGP neighbor status.

```
Device A# show ip bgp neighbors 57.50.1.1
BGP neighbor is 57.50.1.1, remote AS 5750, local AS 23(using Peer's Local AS,
no-prepend, replace-as, dual-as), external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read, hold time is 180, keepalive interval is 60 seconds
  Received 0 messages, 0 notifications, 0 in queue
    open message:0 update message:0 keepalive message:0
    refresh message:0 dynamic cap:0 notifications:0
  Sent 0 messages, 0 notifications, 0 in queue
```

6. Configuration Files

- Device A configuration file

```
!
router bgp 3600
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 57.50.1.1 remote-as 5750
 neighbor 57.50.1.1 local-as 23 no-prepend replace-as dual-as
 neighbor 57.50.1.1 ebgp-multihop 255
 neighbor 57.50.1.1 update-source Loopback 0
 address-family ipv4
  neighbor 57.50.1.1 activate
  exit-address-family
!
```

- Device B configuration file

```
!
router bgp 5750
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 36.0.1.1 remote-as 23
 neighbor 36.0.1.1 ebgp-multihop 255
 neighbor 36.0.1.1 update-source Loopback 0
 address-family ipv4
  neighbor 36.0.1.1 activate
  exit-address-family
!
```

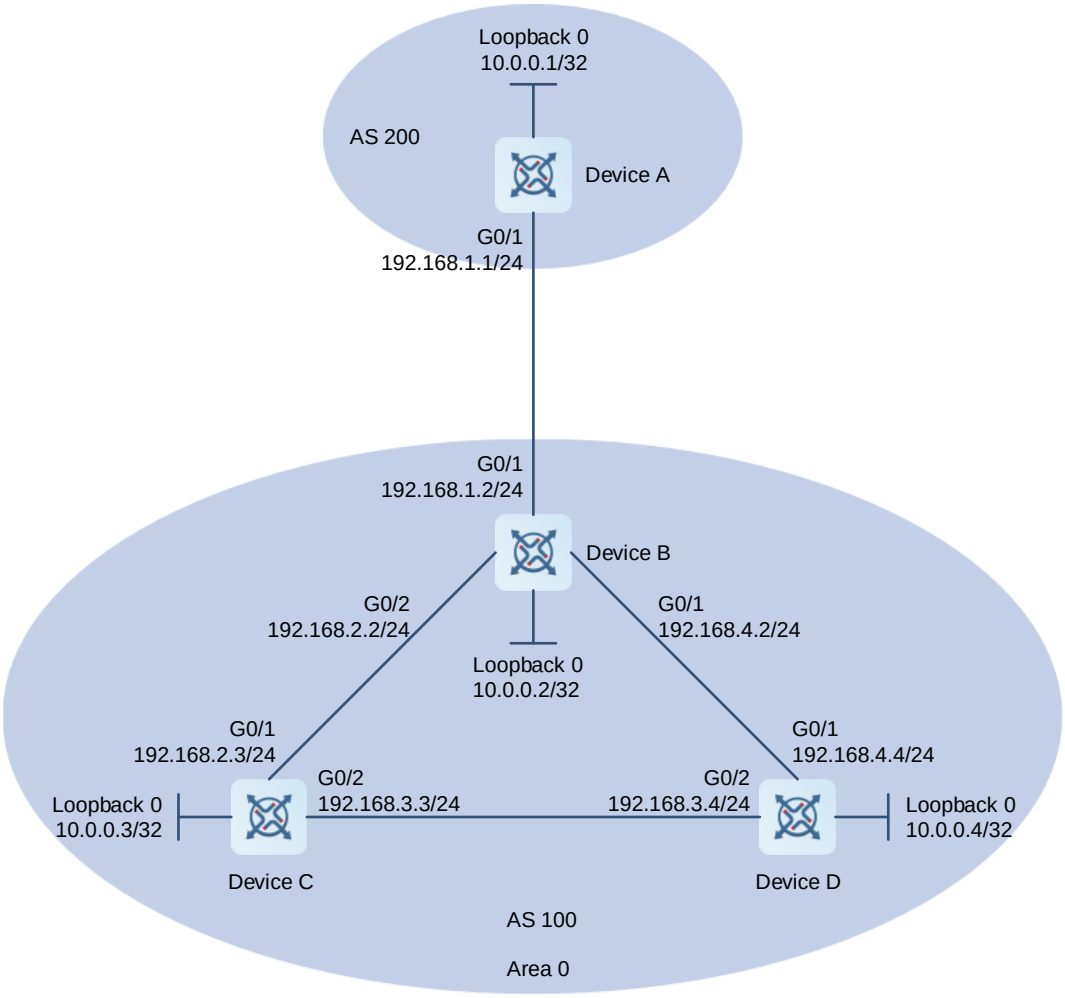
1.11.9 Configuring BGP GR

1. Requirements

Data forwarding should not be interrupted during the protocol restart.

2. Topology

Figure 1-10 Topology of BGP GR



3. Notes

- Enable BGP on all devices and set AS numbers for the devices as shown in Figure 1-10 (omitted).
- Configure a loopback interface on each of devices B, C, and D and configure the devices to establish IBGP neighbor relationships through the loopback interfaces (omitted).
- Configure device As and B to establish an EBGP neighbor relationship through directly connected interfaces (omitted).
- On devices A, B, C, and D, and enable the BGP GR function.

4. Procedure

Configure device A.

```
Device A# configure terminal
```

```
Device A(config)# router ospf 1
Device A(config-router)# graceful-restart
Device A(config-router)# exit
Device A(config)# router bgp 200
Device A(config-router)# bgp graceful-restart
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router ospf 1
Device B(config-router)# graceful-restart
Device B(config-router)# exit
Device B(config)# router bgp 100
Device B(config-router)# bgp graceful-restart
```

Configure device C.

```
Device C# configure terminal
Device C(config)# router ospf 1
Device C(config-router)# graceful-restart
Device C(config-router)# exit
Device C(config)# router bgp 100
Device C(config-router)# bgp graceful-restart
```

Configure device D.

```
Device D# configure terminal
Device D(config)# router ospf 1
Device D(config-router)# graceful-restart
Device D(config-router)# exit
Device D(config)# router bgp 100
Device D(config-router)# bgp graceful-restart
```

5. Verification

On device B, run the **show ip ospf** command to display the OSPF routing status.

```
Device B# show ip ospf
Routing Process "ospf 1" with ID 10.0.0.2
Process uptime is 4 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag isenabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
This router is an ASBR (injecting external routing information)
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
LsaGroupPacing: 240 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 4. Checksum 0x0278E0
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 4
External LSA database is unlimited.
```

```
Number of LSA originated 6
Number of LSA received 2
Log Neighbor Adjency Changes : Enabled
Graceful-restart enabled
Graceful-restart helper support enabled
Number of areas attached to this router: 1
Area 0 (BACKBONE)
```

On device B, run the **show ip bgp neighbors** command to display the BGP neighbor status.

```
Device B# show ip bgp neighbors
BGP neighbor is 192.168.195.183, remote AS 200, local AS 100, external link
Using BFD to detect fast fallover - BFD session state up
  BGP version 4, remote router ID 10.0.0.1
  BGP state = Established, up for 00:06:37
  Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Graceful restart: advertised and received
  Remote Restart timer is 120 seconds
  Address families preserved by peer:
    None
```

6. Configuration Files

- Device A configuration file

```
router bgp 200
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 address-family ipv4
  exit-address-family
!
router ospf 1
 graceful-restart
!
```

- Device B configuration file

```
router bgp 100
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 address-family ipv4
  exit-address-family
!
router ospf 1
```

```
 graceful-restart
!
```

- Device C configuration file

```
router bgp 100
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 address-family ipv4
  exit-address-family
!
router ospf 1
 graceful-restart
!
```

- Device D configuration file

```
router bgp 100
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 address-family ipv4
  exit-address-family
!
router ospf 1
 graceful-restart
!
```

7. Common Errors

- GR is not enabled for IGP.
- GR is not enabled for a BGP neighbor.

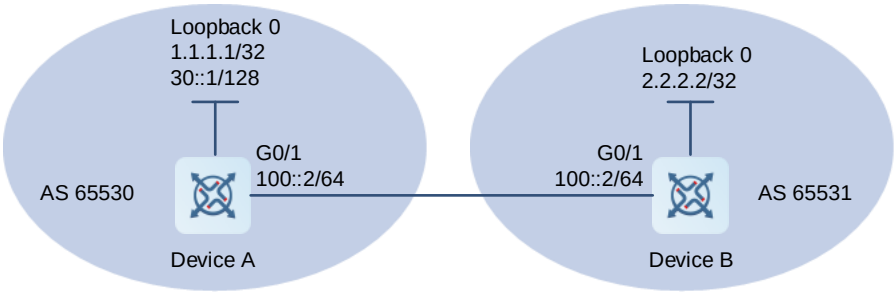
1.11.10 Configuring IPv6 Route Exchange Across ASs

1. Requirements

IPv6 routing information needs to be exchanged across different ASs.

2. Topology

Figure 1-11 Topology of IPv6 Route Exchange Across ASs



3. Notes

- Enable BGP on all devices and set AS numbers for the devices as shown in Figure 1-11 (omitted).
- Configure BGP neighbors, disable the IPv4 address family capability for the neighbors, and activate the IPv6 address family capability.
- Configure BGP to advertise IPv6 routes.

4. Procedure

(1) Configure BGP and activate the IPv6 address family.

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65530
Device A(config-router)# neighbor 100::1 remote-as 65531
Device A(config-router)# address-family ipv4
Device A(config-router-af)# no neighbor 100::1 activate
Device A(config-router-af)# exit-address-family
Device A(config-router)# address-family ipv6
Device A(config-router-af)# neighbor 100::1 activate
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 65531
Device B(config-router)# neighbor 100::2 remote-as 65530
Device B(config-router)# address-family ipv4
Device B(config-router-af)# no neighbor 100::2 activate
Device B(config-router-af)# exit-address-family
Device B(config-router)# address-family ipv6
Device B(config-router-af)# neighbor 100::2 activate
```

(2) Configure the advertisement of IPv6 network information.

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65530
Device A(config-router)# address-family ipv6
Device A(config-router-af)# network 30::1/128
```

5. Verification

On device A, check the BGP neighbor status.

```
Device A# show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 65530
BGP table version is 1
1 BGP AS-PATH entries
0 BGP Community entries
1 BGP Prefix entries (Maximum-prefix:4294967295)
```

```
Neighbor       V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
100::1         4      65531      4      6       1    0    0 00:01:49       0

Total number of neighbors 1
```

On device B, check the BGP neighbor status.

```
Device B# 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, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf     Weight Path
*> 30::1/128        100::2                   0                    0 65530 i

Total number of prefixes 1
```

6. Configuration Files

- Device A configuration file

```
!
router bgp 65530
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 100::1 remote-as 65531
 address-family ipv4
  no neighbor 100::1 activate
  exit-address-family
 address-family ipv6
  network 30::1/128
  neighbor 100::1 activate
  exit-address-family
!
```

- Device B configuration file

```
!
router bgp 65531
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 100::2 remote-as 65530
 address-family ipv4
  no neighbor 100::2 activate
  exit-address-family
```

```
 address-family ipv6
  neighbor 100::2 activate
  exit-address-family
!
```

7. Common Errors

- The IPv6 address family capability is not activated for BGP neighbors.
- In non-6PE scenarios, IPv4 addresses are used to establish a neighbor relationship to exchange IPv6 routes.

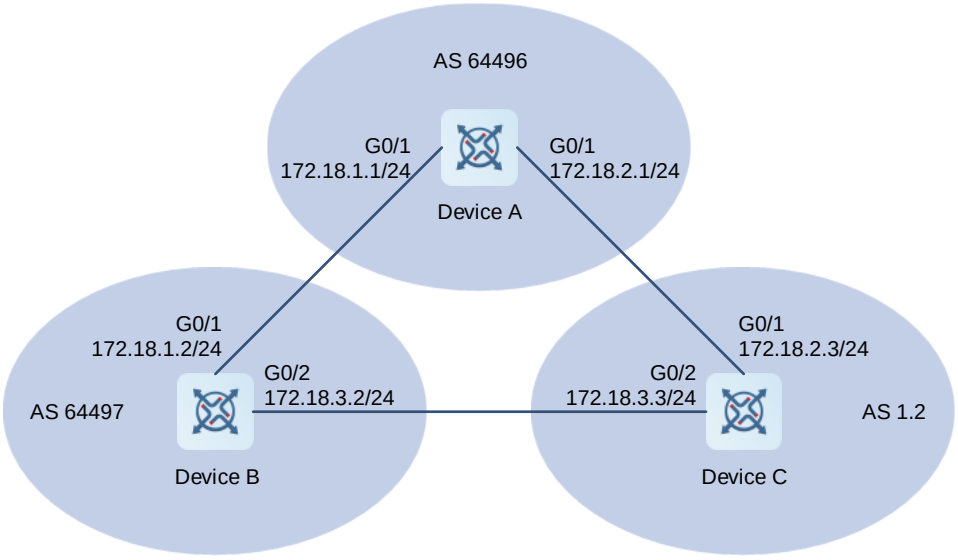
1.11.11 Configuring Compatibility Between BGP Devices Supporting 4-Byte AS Numbers and Those Supporting 2-Byte AS Numbers

1. Requirements

- Routers supporting 2-byte AS numbers and those supporting 4-byte AS numbers (using 2-byte AS numbers) can establish BGP connections.
- Routers supporting 2-byte AS numbers and those supporting 4-byte AS numbers (using 4-byte AS numbers) can establish BGP connections.
- Two routers supporting 4-byte AS numbers can establish a BGP connection, with one using a 2-byte AS number and the other using a 4-byte AS number.

2. Topology

Figure 1-12 Topology of Compatibility Between BGP Devices Supporting 4-Byte AS Numbers and Those Supporting 2-Byte AS Numbers



3. Notes

- Enable BGP on all devices and set AS numbers for the devices as shown in Figure 1-12 (omitted).
- Configure BGP neighbors.

4. Procedure

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 64496
Device A(config-router)# neighbor 172.18.1.2 remote-as 64497
Device A(config-router)# neighbor 172.18.2.3 remote-as 23456
Device A(config-router)# end
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 64497
Device B(config-router)# neighbor 172.18.1.1 remote-as 64496
Device B(config-router)# neighbor 172.18.3.3 remote-as 1.2
Device B(config-router)# bgp asnotation dot
Device B(config-router)# end
```

Configure device C.

```
Device C# configure terminal
Device C(config)# router bgp 1.2
Device C(config-router)# neighbor 172.18.2.1 remote-as 64496
Device C(config-router)# neighbor 172.18.3.2 remote-as 64497
Device C(config-router)# end
```

5. Verification

On device A, check the BGP neighbor status.

```
Device A# show ip bgp summary

BGP router identifier 172.18.1.1, local AS number 64496
BGP table version is 1, main routing table version 1

Neighbor     V   AS      MsgRcvd   MsgSent   TblVer   InQ   OutQ   Up/Down    Statd
172.18.1.2   4   64497   7         7         1        0     0      00:03:04   0
172.18.2.3   4   23456   4         4         1        0     0      00:00:15   0
```

On device B, check the BGP neighbor status.

```
Device B# show ip bgp summary

BGP router identifier 172.18.3.2, local AS number 64497
BGP table version is 1, main routing table version 1

Neighbor     V   AS      MsgRcvd   MsgSent   TblVer   InQ   OutQ   Up/Down    Statd
172.18.1.1   4   64496   7         7         1        0     0      00:00:04   0
172.18.3.2   4   1.2     4         4         1        0     0      00:00:16   0
```

6. Configuration Files

- Device A configuration file

```
!
```

```
router bgp 64496
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 172.18.1.2 remote-as 64497
 neighbor 172.18.2.3 remote-as 23456
 address-family ipv4
  neighbor 172.18.1.2 activate
  neighbor 172.18.2.3 activate
  exit-address-family
!
```

- Device B configuration file

```
!
router bgp 64497
 bgp asnotation dot
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 172.18.1.1 remote-as 64496
 neighbor 172.18.3.3 remote-as 1.2
 address-family ipv4
  neighbor 172.18.1.1 activate
  neighbor 172.18.3.3 activate
  exit-address-family
!
```

- Device C configuration file

```
!
router bgp 65538
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 172.18.2.1 remote-as 64496
 neighbor 172.18.3.2 remote-as 64497
 address-family ipv4
  neighbor 172.18.2.1 activate
  neighbor 172.18.3.2 activate
  exit-address-family
!
```

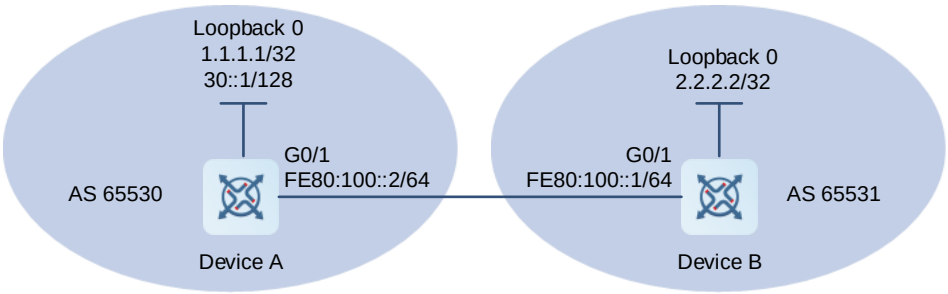
1.11.12 Configuring an IPv6 Local Link Address

1. Requirements

An IPv6 local link address needs to be configured as a neighbor update address.

2. Topology

Figure 1-13 Topology of IPv6 Local Link Address



3. Notes

- Enable BGP on all devices, configure IPv6 local link addresses for interfaces, and set the AS numbers for the devices as shown in Figure 1-13 (omitted).
- Configure BGP neighbors, disable the IPv4 address family capability for the neighbors, and activate the IPv6 address family capability.
- Configure BGP to advertise IPv6 routes.

4. Procedure

(1) Enable the IPv6 address family capability and disable the IPv4 address family capability.

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65530
Device A(config-router)# neighbor fe80:100::1%Gi0/1 remote-as 65531
Device A(config-router)# address-family ipv4
Device A(config-router-af)# no neighbor fe80:100::1%Gi0/1 activate
Device A(config-router-af)# exit-address-family
Device A(config-router)# address-family ipv6
Device A(config-router-af)# neighbor fe80:100::1%Gi0/1 activate
Device A(config-router-af)# network 30::1/128
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 65531
Device B(config-router)# neighbor fe80:100::2%Gi0/1 remote-as 65530
Device B(config-router)# address-family ipv4
Device B(config-router-af)# no neighbor fe80:100::2%Gi0/1 activate
Device B(config-router-af)# exit-address-family
Device B(config-router)# address-family ipv6
Device B(config-router-af)# neighbor fe80:100::2%Gi0/1 activate
```

(2) Configure BGP to advertise IPv6 addresses.

Configure device A.

```
Device A# configure terminal
```

```
Device A(config)# router bgp 65530
Device A(config-router)# address-family ipv6
Device A(config-router-af)# network 30::1/128
```

5. Verification

On device A, check the BGP neighbor status.

```
Device A# show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 65530
BGP table version is 1
1 BGP AS-PATH entries
0 BGP Community entries
1 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor            V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
fe80:100::1%Gi0/1    4      65531      4      6       1    0    0 00:01:49
0

Total number of neighbors 1
```

On device B, check the BGP neighbor status.

```
Device B# 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, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf     Weight Path
*> 30::1/128        fe80:100::2          0                     0 65530 i

Total number of prefixes 1
```

6. Configuration Files

- Device A configuration file

```
!
router bgp 65530
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor fe80:100::1%Gi0/1 remote-as 65531
 address-family ipv4
  no neighbor fe80:100::1%Gi0/1 activate
  exit-address-family
 address-family ipv6
  network 30::1/128
  neighbor fe80:100::1%Gi0/1 activate
```

```
  exit-address-family
!
```

- Device B configuration file

```
!
router bgp 65531
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor fe80:100::2%Gi0/1 remote-as 65530
 address-family ipv4
  no neighbor fe80:100::2%Gi0/1 activate
  exit-address-family
 address-family ipv6
  neighbor fe80:100::2%Gi0/1 activate
  exit-address-family
!
```

7. Common Errors

- An IPv6 local link address is used to establish a neighbor relationship during neighbor configuration, but the interface, on which the IPv6 local link address is configured, is not configured as the update source during local configuration.
- Only one end uses an IPv6 local link address for establishing a neighbor relationship.

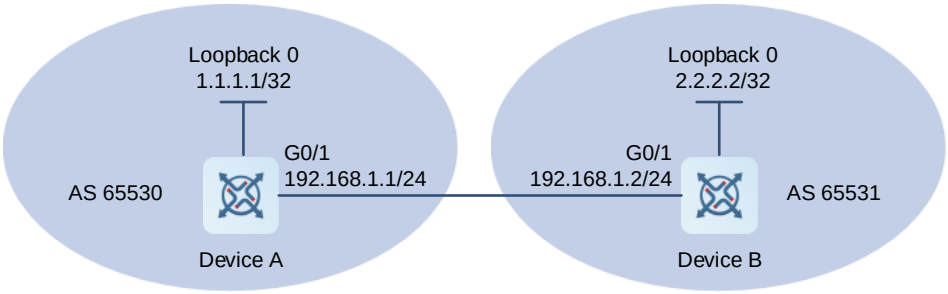
1.11.13 Configuring BGP NSR

1. Requirements

NSR can be configured to ensure that data switching and forwarding are not interrupted.

2. Topology

Figure 1-14 Topology of BGP NSR



3. Notes

- Enable BGP on all devices and set AS numbers for the devices as shown in Figure 1-14 (omitted).
- Configure devices A and B to establish an EBGP neighbor relationship through directly connected interfaces.
- Enable the BGP NSR function on device A.

4. Procedure

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65530
Device A(config-router)# neighbor 192.168.1.2 remote-as 65530
Device A(config-router)# neighbor 192.168.1.2 ha-mode nsr
```

5. Verification

On device A, check the BGP neighbor status.

```
Device A# show ip bgp neighbors
BGP neighbor is 192.168.1.2, remote AS 65530, local AS 65531, external link
Using BFD to detect fast fallover - BFD session state up
  BGP version 4, remote router ID 2.2.2.2
  BGP state = Established, up for 00:06:37
  Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Graceful restart: advertised and received
  Remote Restart timer is 120 seconds
  Address families preserved by peer:
    None
```

On device B, check the BGP neighbor status.

```
Device B# show ip bgp neighbors
BGP neighbor is 192.168.1.1, remote AS 65530, local AS 65531, external link
Using BFD to detect fast fallover - BFD session state up
  BGP version 4, remote router ID 1.1.1.1
  BGP state = Established, up for 00:06:37
  Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Graceful restart: advertised and received
  Remote Restart timer is 120 seconds
  Address families preserved by peer:
    None
```

6. Configuration Files

- Device A configuration file

```
!
router bgp 65530
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
```

```
bgp nsr
neighbor 192.168.1.2 remote-as 65530
address-family ipv4
 neighbor 192.168.1.2 activate
 exit-address-family
!
```

7. Common Errors

- IGP is not configured.
- The NSR function is not enabled for BGP neighbors.

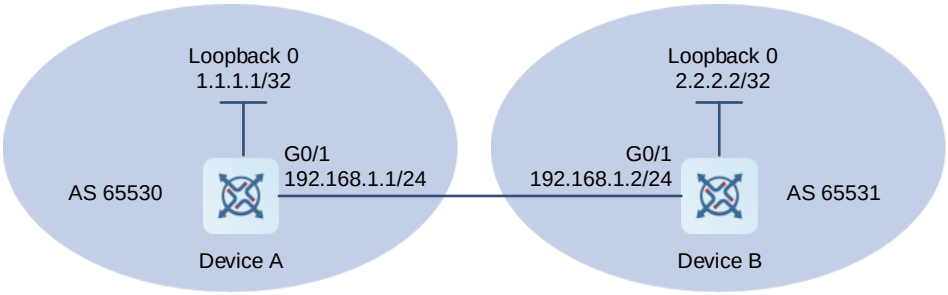
1.11.14 Configuring BGP Routes to Be Recursive Only to Host Routes

1. Requirements

Non-direct BGP routes need to be recursive to host routes.

2. Topology

Figure 1-15 Topology of Configuring BGP Routes to Be Recursive Only to Host Routes



3. Notes

- Enable BGP on all devices and set the AS numbers as shown in the figure above (omitted).
- Configure devices A and B to establish an EBGP neighbor relationship through loopback interfaces (omitted).
- On devices A and B, enable the function of making BGP routes recursive only to host routes.

4. Procedure

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65530
Device A(config-router)# bgp recursion host
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 65531
Device B(config-router)# bgp recursion host
```

5. Configuration Files

- Device A configuration file

```
!
router bgp 65530
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 address-family ipv4
  bgp recursion host
  exit-address-family
!
```

- Device B configuration file

```
!
router bgp 65531
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 address-family ipv4
  bgp recursion host
  exit-address-family
!
```

6. Common Errors

If an IBGP or multi-hop EBGP neighbor relationship is established not using loopback addresses, after the function is enabled, BGP cannot to find host routes matching the next-hop addresses. As a result, the next hops of BGP routes are invalid and routes cannot be preferentially selected.

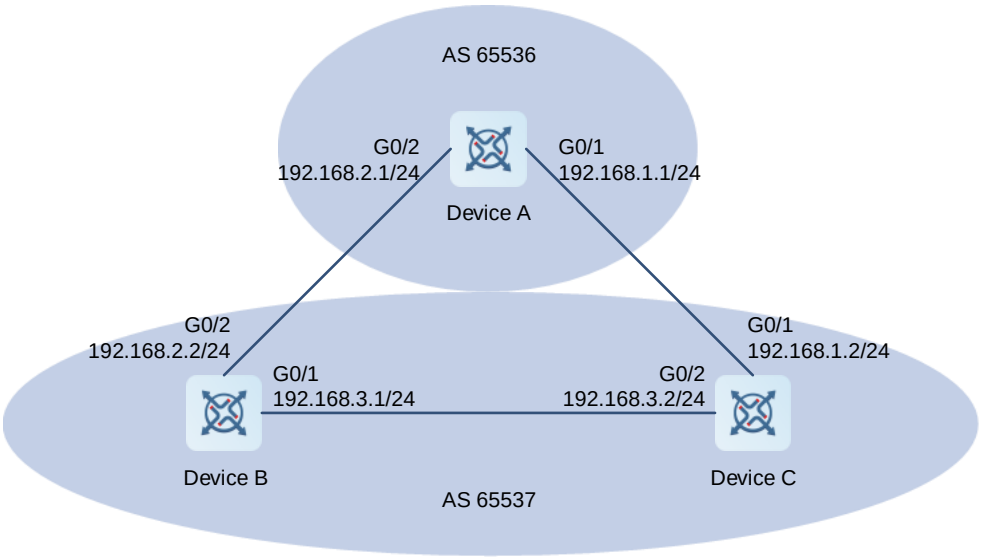
1.11.15 Configuring Outbound Loop Detection for a BGP Neighbor

1. Requirements

Outbound loop detection needs to be configured for a BGP neighbor to prevent the receiving of routing information carrying the AS number of the neighbor in the **AS-PATH** attribute.

2. Topology

Figure 1-16 Topology of Outbound Loop Detection for a BGP Neighbor



3. Notes

- Enable BGP on all devices and set AS numbers for the devices as shown in Figure 1-16 (omitted).
- Configure devices A and C and devices B and C to establish EBGP neighbor relationships (omitted).
- On device C, enable outbound loop detection for its neighbors: devices A and B.

4. Procedure

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65536
Device A(config-router)# neighbor 192.168.1.2 remote-as 65537
Device A(config-router)# neighbor 192.168.1.2 as-loop-check out
Device A(config-router)# neighbor 192.168.2.2 remote-as 65537
Device A(config-router)# neighbor 192.168.2.2 as-loop-check out
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 65537
Device B(config-router)# neighbor 192.168.2.1 remote-as 65536
Device B(config-router)# neighbor 192.168.3.2 remote-as 65537
```

Configure device C.

```
Device C# configure terminal
Device C(config)# router bgp 65537
Device C(config-router)# neighbor 192.168.1.1 remote-as 65536
Device C(config-router)# neighbor 192.168.3.1 remote-as 65537
```

5. Verification

On device A, check the BGP neighbor status.

```
Device A# show ip bgp neighbors 192.168.2.2
BGP neighbor is 192.168.2.2, remote AS 65537, local AS 65536, external link
Using as path loop detection in announcing route
  BGP version 4, remote router ID 192.168.2.2
  BGP state = Established, up for 00:06:37
  Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Graceful restart: advertised and received
  Remote Restart timer is 120 seconds
  Address families preserved by peer:
    None
......
```

6. Configuration Files

- Device A configuration file

```
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.1.2 remote-as 65537
 neighbor 192.168.2.2 remote-as 65537
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 as-loop-check out
  neighbor 192.168.2.2 activate
  neighbor 192.168.2.2 as-loop-check out
  exit-address-family
!
```

- Device B configuration file

```
!
router bgp 65537
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.2.1 remote-as 65536
 neighbor 192.168.3.2 remote-as 65537
 address-family ipv4
  neighbor 192.168.2.1 activate
  neighbor 192.168.3.2 activate
  exit-address-family
```

```
!
```

- Device C configuration file

```
!
router bgp 65537
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.1.1 remote-as 65536
 neighbor 192.168.3.1 remote-as 65537
 address-family ipv4
  neighbor 192.168.1.1 activate
  neighbor 192.168.3.1 activate
  exit-address-family
!
```

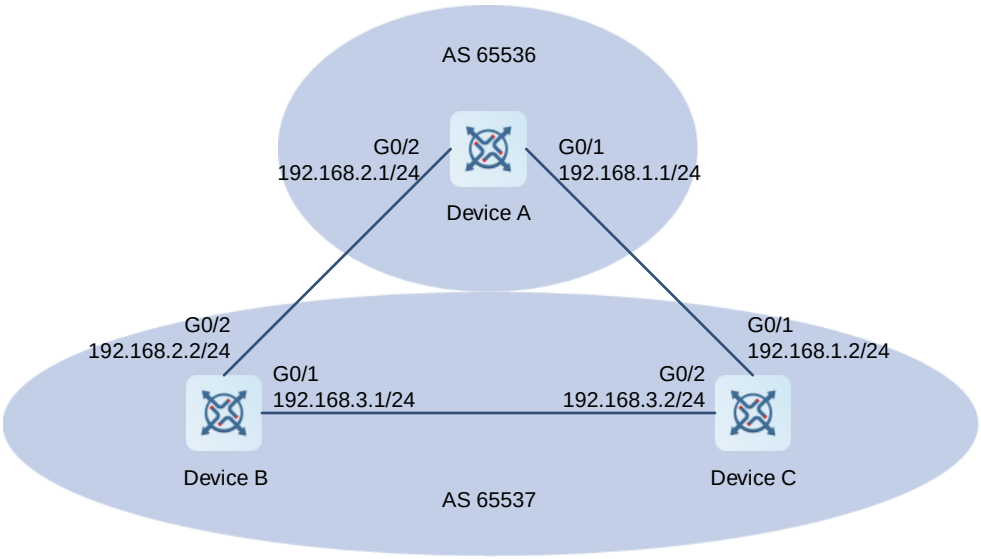
1.11.16 Shutting Down BGP Connections Gracefully

1. Requirements

Graceful shutdown of BGP connections needs to be configured on a device. Then, after a certain period of time (automatically calculated based on the number of advertised routes or specified by *delay time*), the device disconnects BGP connections from its neighbors to reduce the impact on the network.

2. Topology

Figure 1-17 Topology of Graceful Shutdown of BGP Connections



3. Notes

- Enable BGP on all devices and set AS numbers for the devices as shown in Figure 1-17 (omitted).
- Configure devices A and C and devices B and C to establish EBGP neighbor relationships (omitted).
- On device A, configure the graceful shutdown of all connections in the BGP instance.

4. Procedure

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 65536
Device A(config-router)# neighbor 192.168.1.2 remote-as 65537
Device A(config-router)# neighbor 192.168.1.2 as-loop-check out
Device A(config-router)# neighbor 192.168.2.2 remote-as 65537
Device A(config-router)# neighbor 192.168.2.2 as-loop-check out
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 65537
Device B(config-router)# neighbor 192.168.2.1 remote-as 65536
Device B(config-router)# neighbor 192.168.3.2 remote-as 65537
```

Configure device C.

```
Device C# configure terminal
Device C(config)# router bgp 65537
Device C(config-router)# neighbor 192.168.1.1 remote-as 65536
Device C(config-router)# neighbor 192.168.3.1 remote-as 65537
Device C(config-router)# bgp shutdown graceful
```

5. Verification

On device C, check the BGP neighbor status.

```
Device C(config)#show ip bgp neighbor 192.168.1.1
For address family: IPv4 Unicast
BGP neighbor is 192.168.1.1, remote AS 65536, local AS 65537, external link
 Administratively graceful shut down
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read        , hold time is 30, keepalive interval is 1 seconds
  Configured hold time is 30, keepalive interval is 1 seconds
  Received 0 messages, 0 notifications, 0 in queue
    open message:0 update message:0 keepalive message:0
    refresh message:0 dynamic cap:0 notifications:0
  Sent 0 messages, 0 notifications, 0 in queue
    open message:0 update message:0 keepalive message:0
    refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Update source is Loopback 0

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes
  0 announced prefixes
```

```
 Connections established 0; dropped 0
  BGP neighbor may be up to 255 hops away.
Sock_fd: -1
Last Reset:        , due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)
```

6. Configuration Files

- Device A configuration file

```
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.1.2 remote-as 65537
 neighbor 192.168.2.2 remote-as 65537
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 as-loop-check out
  neighbor 192.168.2.2 activate
  neighbor 192.168.2.2 as-loop-check out
  exit-address-family
!
```

- Device B configuration file

```
!
router bgp 65537
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.2.1 remote-as 65536
 neighbor 192.168.3.2 remote-as 65537
 address-family ipv4
  neighbor 192.168.2.1 activate
  neighbor 192.168.3.2 activate
  exit-address-family
!
```

- Device C configuration file

```
!
router bgp 65537
 bgp shutdown graceful
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
```

```
 bgp graceful-restart
 neighbor 192.168.1.1 remote-as 65536
 neighbor 192.168.3.1 remote-as 65537
 address-family ipv4
  neighbor 192.168.1.1 activate
  neighbor 192.168.3.1 activate
  exit-address-family
!
```

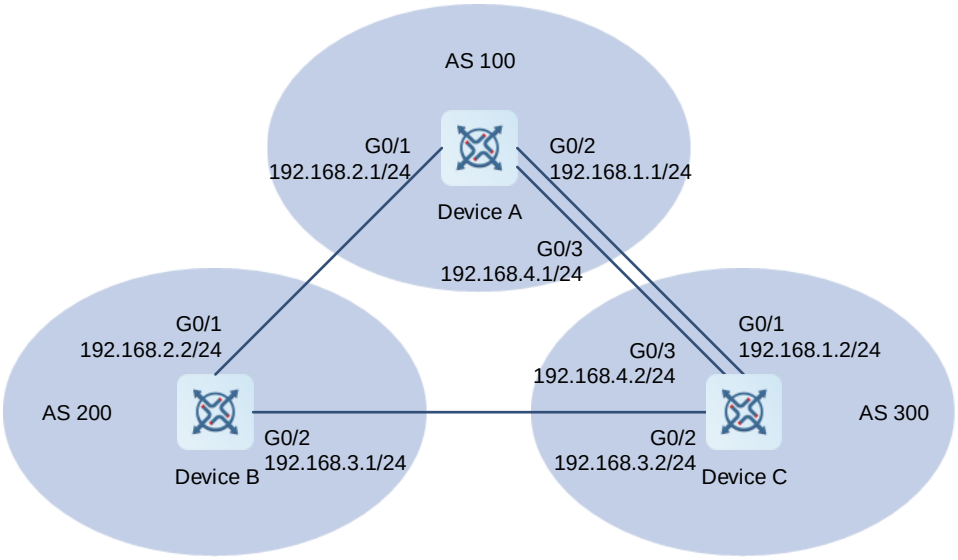
1.11.17 Configuring BGP Multi-Path Bypass Protection

1. Requirements

Multi-path bypass protection needs to be configured to enhance routing reliability.

2. Topology

Figure 1-18 Topology of BGP Multi-Path Bypass Protection



3. Notes

- Enable BGP on all devices (omitted).
- Configure addresses for directly connected interfaces on devices A, B, and C, and configure them to establish EBGP neighbor relationships (omitted).
- Configure a BFD session for the EBGP neighbor relationship between devices A and C (omitted).
- On device C, configure BGP multi-path bypass protection and ECMP.

4. Procedure

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 100
Device A(config-router)# neighbor 192.168.1.2 remote-as 300
Device A(config-router)# neighbor 192.168.4.2 remote-as 300
```

```
Device A(config-router)# neighbor 192.168.2.2 remote-as 200
Device A(config-router)# maximum-paths ebgp 2
Device A(config-router)# redistribute connect
```

Configure device B.

```
Device B# configure terminal
Device B(config)# router bgp 200
Device B(config-router)# neighbor 192.168.3.2 remote-as 300
Device B(config-router)# neighbor 192.168.3.2 fall-over bfd
Device B(config-router)# neighbor 192.168.2.1 remote-as 100
Device B(config-router)# redistribute connect
```

Configure device C.

```
Device C# configure terminal
Device C(config)# router bgp 300
Device C(config-router)# neighbor 192.168.1.1 remote-as 100
Device C(config-router)# neighbor 192.168.4.1 remote-as 100
Device C(config-router)# neighbor 192.168.3.1 remote-as 200
Device C(config-router)# neighbor 192.168.1.1 fall-over bfd
Device C(config-router)# neighbor 192.168.4.1 fall-over bfd
Device C(config-router)# maximum-paths ebgp 2
Device C(config-router)# address-family ipv4 unicast
Device C(config-router-af)# bgp install standby-path
Device C(config-router-af)# redistribute connect
```

5. Verification

On device C, check BGP information.

```
Device C# show ip bgp summary
BGP router identifier 192.168.4.2, local AS number 300
BGP table version is 12
4 BGP AS-PATH entries
0 BGP Community entries
4 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor       V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
192.168.1.1    4        100     76     77      12    12    0 00:59:27       3
192.168.3.1    4        200     30     30      12    12    0 00:19:03       3
192.168.4.1    4        100     76     77      12    12    0 00:59:01       3

Total number of neighbors 3

Device C# show ip bgp
BGP table version is 12, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry, m - multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network          Next Hop          Metric     LocPrf     Weight Path
*  192.168.1.0      192.168.3.1            0                    0 200 ?
*                 192.168.4.1            0                    0 100 ?
*                 192.168.1.1            0                    0 100 ?
*>                0.0.0.0                0                32768    ?
*> 192.168.2.0      192.168.4.1            0                    0 200 ?
*m                192.168.1.1            0                    0 200 ?
*b                192.168.3.1            0                    0 100 ?
*  192.168.3.0      192.168.3.1            0                    0 200 ?
*                 192.168.4.1            0                    0 100 200 ?
*                 192.168.1.1            0                    0 100 200 ?
*>                0.0.0.0                0                32768    ?
*  192.168.4.0      192.168.3.1            0                    0 200 ?
*                 192.168.4.1            0                    0 100 ?
*                 192.168.1.1            0                    0 100 ?
*>                0.0.0.0                0                32768    ?

Total number of prefixes 4
Device C# show ip bgp 192.168.2.0
BGP routing table entry for 192.168.2.0/24
Paths: (3 available, best #3, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  192.168.1.1
  200
    192.168.3.1 from 192.168.3.1 (3.3.3.3)
      Origin incomplete, metric 0, localpref 100, valid, external, backup
      Last update: Tue Oct  5 00:26:52 1971

  100
    192.168.1.1 from 192.168.1.1 (44.44.44.44)
      Origin incomplete, metric 0, localpref 100, valid, external, multipath
      Last update: Mon Oct  4 23:46:28 1971

  100
    192.168.4.1 from 192.168.4.1 (44.44.44.44)
      Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
      Last update: Mon Oct  4 23:46:28 1971
Device C# show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
```

```
Gateway of last resort is no set
C   192.168.1.0/24 is directly connected, GigabitEthernet 0/1
C   192.168.1.2/32 is local host.
B   192.168.2.0/24 [20/0] via 192.168.1.1, 00:21:39
                [20/0] via 192.168.4.1, 00:21:39
C   192.168.3.0/24 is directly connected, GigabitEthernet 0/2
C   192.168.3.2/32 is local host.
C   192.168.4.0/24 is directly connected, GigabitEthernet 0/3
C   192.168.4.2/32 is local host.
```

6. Configuration Files

- Device A configuration file

```
!
router bgp 100
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.1.2 remote-as 300
 neighbor 192.168.2.2 remote-as 200
 neighbor 192.168.4.2 remote-as 300
 address-family ipv4
  maximum-paths ebgp 2
  redistribute connected
  neighbor 192.168.1.2 activate
  neighbor 192.168.2.2 activate
  neighbor 192.168.4.2 activate
  exit-address-family
!
```

- Device B configuration file

```
!
router bgp 200
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.2.1 remote-as 100
 neighbor 192.168.3.2 remote-as 300
 neighbor 192.168.3.2 fall-over bfd
 address-family ipv4
  redistribute connected
  neighbor 192.168.2.1 activate
  neighbor 192.168.3.2 activate
  exit-address-family
```

```
!
```

- Device C configuration file

```
!
router bgp 300
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.1.1 remote-as 100
 neighbor 192.168.1.1 fall-over bfd
 neighbor 192.168.3.1 remote-as 200
 neighbor 192.168.4.1 remote-as 100
 neighbor 192.168.4.1 fall-over bfd
 address-family ipv4
  maximum-paths ebgp 2
  bgp install standby-path
  redistribute connected
  neighbor 192.168.1.1 activate
  neighbor 192.168.3.1 activate
  neighbor 192.168.4.1 activate
  exit-address-family
!
```

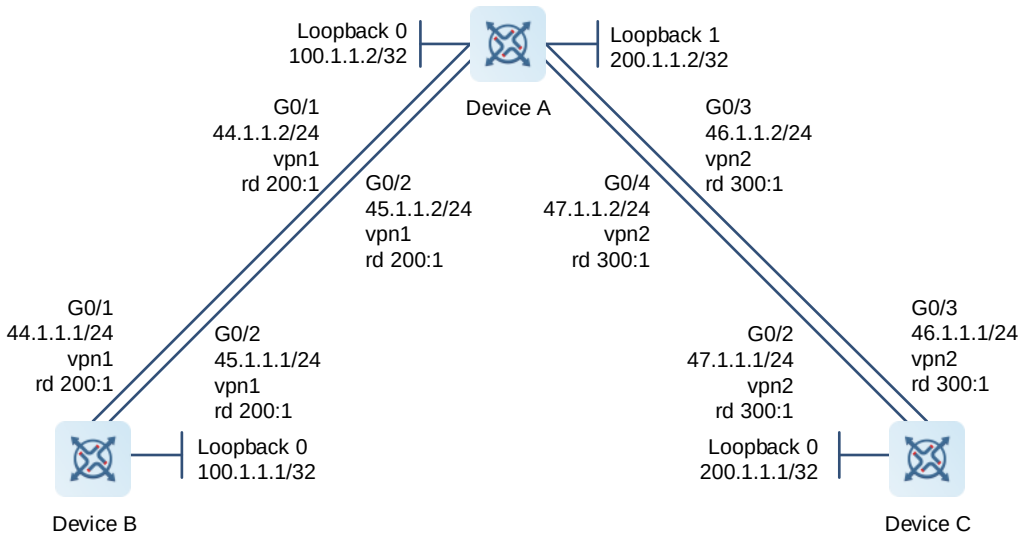
1.11.18 Configuring Multi-Path Route Import Between VRF Instances

1. Requirements

Device A is connected with two networks through the interfaces of two VRF instances (vpn1 and vpn2) so that cross-VRF access is implemented through device A.

2. Topology

Figure 1-19 Topology of Multi-Path Route Import Between VRF Instances



3. Notes

- Configure VRF instances and VRF static routes.
- Configure a VRF address family.
- Import VRF static routes to BGP.
- Enable the function of importing multi-path static routes to BGP.
- Configure BGP ECMP.
- Configure the import of all path routes between VRF instances.

4. Procedure

(1) Configure VRF instances and VRF static routes.

Configure device A.

```
Device A# configure terminal
Device A(config)# ip vrf vpn1
Device A(config-vrf)# rd 200:1
Device A(config-vrf)# route-target both 100:100
Device A(config-vrf)# exit
Device A(config)# ip vrf vpn2
Device A(config-vrf)# rd 300:1
Device A(config-vrf)# route-target both 100:100
Device A(config-vrf)# exit
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip vrf forwarding vpn1
Device A(config-if-GigabitEthernet 0/1)# ip address 44.1.1.2 255.255.255.0
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface GigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ip vrf forwarding vpn1
Device A(config-if-GigabitEthernet 0/2)# ip address 45.1.1.2 255.255.255.0
Device A(config-if-GigabitEthernet 0/2)# exit
Device A(config)# interface GigabitEthernet 0/3
Device A(config-if-GigabitEthernet 0/3)# ip vrf forwarding vpn2
Device A(config-if-GigabitEthernet 0/3)# ip address 46.1.1.2 255.255.255.0
Device A(config-if-GigabitEthernet 0/3)# exit
Device A(config)# interface GigabitEthernet 0/4
Device A(config-if-GigabitEthernet 0/4)# ip vrf forwarding vpn2
Device A(config-if-GigabitEthernet 0/4)# ip address 47.1.1.2 255.255.255.0
Device A(config-if-GigabitEthernet 0/4)# exit
Device A(config)# ip route vrf vpn1 100.1.1.1 255.255.255.255 44.1.1.1
Device A(config)# ip route vrf vpn1 100.1.1.1 255.255.255.255 45.1.1.1
Device A(config)# ip route vrf vpn2 200.1.1.1 255.255.255.255 46.1.1.1
Device A(config)# ip route vrf vpn2 200.1.1.1 255.255.255.255 47.1.1.1
```

Configure device B.

```
Device B# configure terminal
Device B(config)# ip vrf vpn1
Device B(config-vrf)# rd 200:1
```

```
Device B(config-vrf)# route-target both 100:100
Device B(config-vrf)# exit
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip vrf forwarding vpn1
Device B(config-if-GigabitEthernet 0/1)# ip address 44.1.1.1 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ip vrf forwarding vpn1
Device B(config-if-GigabitEthernet 0/2)# ip address 45.1.1.1 255.255.255.0
Device B(config-if-GigabitEthernet 0/2)# exit
Device B(config)# ip route vrf vpn1 100.1.1.2 255.255.255.255 44.1.1.2
Device B(config)# ip route vrf vpn1 100.1.1.2 255.255.255.255 45.1.1.2
```

Configure device C.

```
Device C# configure terminal
Device C(config)# ip vrf vpn2
Device C(config-vrf)# rd 300:1
Device C(config-vrf)# route-target both 100:100
Device C(config-vrf)# exit
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip vrf forwarding vpn2
Device C(config-if-GigabitEthernet 0/1)# ip address 46.1.1.1 255.255.255.0
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface GigabitEthernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ip vrf forwarding vpn2
Device C(config-if-GigabitEthernet 0/2)# ip address 47.1.1.1 255.255.255.0
Device C(config-if-GigabitEthernet 0/2)# exit
Device C(config)# ip route vrf vpn2 200.1.1.2 255.255.255.255 46.1.1.2
Device C(config)# ip route vrf vpn2 200.1.1.2 255.255.255.255 47.1.1.2
```

(2) Configure the function of importing multi-path static routes to BGP to implement inter-VRF route import.

Configure device A.

```
Device A# configure terminal
Device A(config)# router bgp 100
Device A(config-router)# address-family ipv4 vrf vpn1
Device A(config-router-af)# redistribute static
Device A(config-router-af)# maximum-paths ebgp 32
Device A(config-router-af)# bgp sourced-paths static all
Device A(config-router-af)# import path selection all
Device A(config-router-af)# exit-address-family
Device A(config-router)# address-family ipv4 vrf vpn2
Device A(config-router-af)# redistribute static
Device A(config-router-af)# maximum-paths ebgp 32
Device A(config-router-af)# bgp sourced-paths static all
Device A(config-router-af)# import path selection all
Device A(config-router-af)# exit-address-family
```

5. Verification

On device A, check VRF routes.

```
Device A# show ip route vrf vpn1
Routing Table: vpn1

Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, A - Arp to host
       * - candidate default

Gateway of last resort is no set
C    44.1.1.0/24 is directly connected, GigabitEthernet 0/1
C    44.1.1.2/32 is local host.
C    45.1.1.0/24 is directly connected, GigabitEthernet 0/2
C    45.1.1.2/32 is local host.
S    100.1.1.1/32 [1/0] via 44.1.1.1
                [1/0] via 45.1.1.1
B    200.1.1.1/32 [20/0] via 47.1.1.1, 02:32:01
                [20/0] via 46.1.1.1, 02:32:01

Device A# show ip route vrf vpn2
Routing Table: vpn2

Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, A - Arp to host
       * - candidate default

Gateway of last resort is no set
C    46.1.1.0/24 is directly connected, GigabitEthernet 0/3
C    46.1.1.2/32 is local host.
C    47.1.1.0/24 is directly connected, GigabitEthernet 0/4
C    47.1.1.2/32 is local host.
B    100.1.1.1/32 [20/0] via 45.1.1.1, 03:27:07
                [20/0] via 44.1.1.1, 03:27:07
S    200.1.1.1/32 [1/0] via 46.1.1.1
                [1/0] via 47.1.1.1
```

6. Configuration Files

- Device A configuration file

```
!
ip vrf vpn1
 rd 200:1
 route-target both 100:100
!
ip vrf vpn2
 rd 300:1
 route-target both 100:100
!
interface GigabitEthernet 0/1
 no switchport
 ip vrf forwarding vpn1
 ip address 44.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip vrf forwarding vpn1
 ip address 45.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip vrf forwarding vpn2
 ip address 46.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/4
 no switchport
 ip vrf forwarding vpn2
 ip address 47.1.1.2 255.255.255.0
!
router bgp 100
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 address-family ipv4
  exit-address-family
  !
 address-family ipv4 vrf vpn1
  maximum-paths ebgp 32
  bgp sourced-paths static all
  import path selection all
  redistribute static
  exit-address-family
  !
 address-family ipv4 vrf vpn2
  maximum-paths ebgp 32
```

```
 bgp sourced-paths static all
 import path selection all
 redistribute static
 exit-address-family
!
ip route vrf vpn1 100.1.1.1 255.255.255.255 44.1.1.1
ip route vrf vpn1 100.1.1.1 255.255.255.255 45.1.1.1
ip route vrf vpn2 200.1.1.1 255.255.255.255 46.1.1.1
ip route vrf vpn2 200.1.1.1 255.255.255.255 47.1.1.1
!
```

- Device B configuration file

```
!
ip vrf vpn1
 rd 200:1
 route-target both 100:100
!
interface GigabitEthernet 0/1
 no switchport
 ip vrf forwarding vpn1
 ip address 44.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip vrf forwarding vpn1
 ip address 45.1.1.1 255.255.255.0
!
ip route vrf vpn1 100.1.1.2 255.255.255.255 44.1.1.2
ip route vrf vpn1 100.1.1.2 255.255.255.255 45.1.1.2
!
```

- Device C configuration file

```
!
ip vrf vpn2
 rd 300:1
 route-target both 100:100
!
interface GigabitEthernet 0/1
 no switchport
 ip vrf forwarding vpn2
 ip address 46.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip vrf forwarding vpn2
 ip address 47.1.1.1 255.255.255.0
!
```

```
ip route vrf vpn2 200.1.1.2 255.255.255.255 46.1.1.2
ip route vrf vpn2 200.1.1.2 255.255.255.255 47.1.1.2
!
```

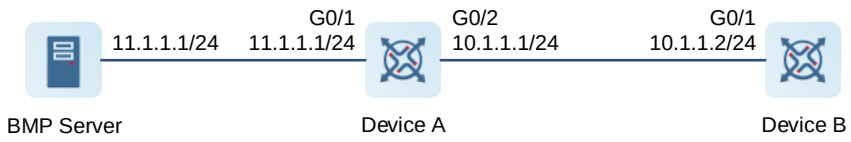
1.11.19 Configuring BMP Monitoring

1. Requirements

The BGP connections established between devices A and B need to be monitored by the BMP server.

2. Topology

Figure 1-20 Topology of BMP Monitoring



3. Notes

- Configure BGP basic features (omitted).
- Configure information relevant to a BMP server instance (address, port number, and type of monitored routes).
- Configure the BMP server to monitor BGP peers.

4. Procedure

(1) Configure information related to a BMP server instance.

Configure device A.

```
Device A# configure
Device A(config)# bmp server 1
Device A(config-bmpsrvr)# address 11.1.1.2 port 12345
Device A(config-bmpsrvr)# update-source gigabitEthernet 0/1
Device A(config-bmpsrvr)# adj-rib-in post-policy
```

(2) Configure the BMP server to monitor BGP peers.

Configure device A.

```
Device A(config)# router bgp 100
Device A(config-router)# neighbor 10.1.1.2 remote-as 100
Device A(config-router)# neighbor 10.1.1.2 bmp-active server 1
```

5. Verification

On device A, check BGP information.

```
Device A# show bgp all summary
For address family: IPv4 Unicast
BGP router identifier 11.1.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP Community entries
```

```
25 BGP Prefix entries (Maximum-prefix:262144)

Neighbor       V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.1.1.2       4        100      0      0       0    0    0 05:36:32      23

Device A# show bgp bmp neighbor

Neighbor       CfgSvr#          ActSvr#
10.1.1.2       1               1

Device A# show bgp bmp summary
ID   Host               Port    State       Time       NBRs
1    11.1.1.2           12345    Established  05:36:12    1
```

6. Configuration Files

- Device A configuration file

```
!
router bgp 100
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.2 remote-as 100
 neighbor 10.1.1.2 bmp-active server 1
 address-family ipv4
  neighbor 10.1.1.2 activate
  exit-address-family
!
bmp server 1
 address 11.1.1.2 port 12345
 update-source GigabitEthernet 0/1
 adj-rib-in post-policy
!
```

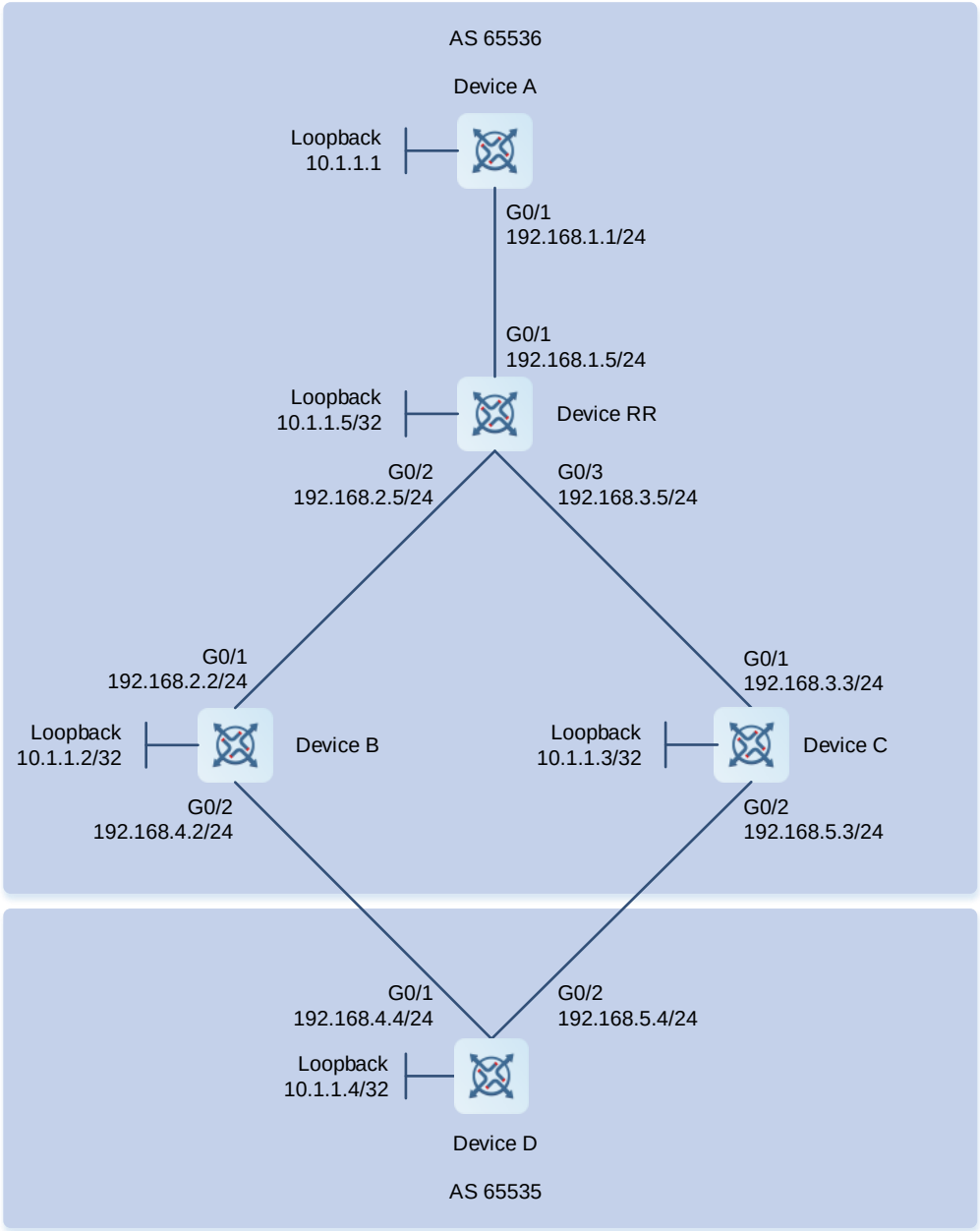
1.11.20 Configuring BGP ADD-PATH

1. Requirements

When the device is allowed to advertise multiple routes with the same prefix to a neighbor, you can define ADD-PATH to enable multiple links to implement load sharing or backup, thereby increasing the network link reliability.

2. Topology

Figure 1-21 Topology of the BGP ADD-PATH



3. Notes

- As shown in Figure 1-21, configure interconnection addresses for devices A, B, C, D, and RR, configure devices A, B, C, and RR to establish IBGP neighbor relationships, configure device RR as a BGP route reflector, and configure devices B and D and devices C and D to establish EBGP neighbor relationships.
- Configure a loopback address on device D and advertise it to BGP.
- Configure the ADD-PATH advertisement capability on device RR and the ADD-PATH receiving capability on device A.

4. Procedure

(1) Configure BGP basic features and interface IP addresses on devices A, B, C, and D.

Configure device A.

```
Device A# configure terminal
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# router bgp 65536
Device A(config-router)# neighbor 192.168.1.5 remote-as 65536
Device A(config-router)# neighbor 192.168.1.5 additional-paths receive
```

Configure device B.

```
Device B# configure terminal
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ip address 192.168.4.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/2)# exit
Device B(config)# router bgp 65536
Device B(config-router)# neighbor 192.168.2.5 remote-as 65536
Device B(config-router)# neighbor 192.168.4.4 remote-as 65535
```

Configure device C.

```
Device C# configure terminal
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip address 192.168.3.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface GigabitEthernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ip address 192.168.5.3 255.255.255.0
Device C(config-if-GigabitEthernet 0/2)# exit
Device C(config)# router bgp 65536
Device C(config-router)# neighbor 192.168.3.5 remote-as 65536
Device C(config-router)# neighbor 192.168.5.4 remote-as 65535
```

Configure device D.

```
Device D# configure terminal
Device D(config)# interface loopback 0
Device D(config-if-Loopback 0)# ip address 10.1.1.4 255.255.255.255
Device D(config-if-Loopback 0)# exit
Device D(config)# interface GigabitEthernet 0/1
Device D(config-if-GigabitEthernet 0/1)# ip address 192.168.4.4 255.255.255.0
Device D(config-if-GigabitEthernet 0/1)# exit
Device D(config)# interface GigabitEthernet 0/1
Device D(config-if-GigabitEthernet 0/1)# ip address 192.168.5.4 255.255.255.0
Device D(config-if-GigabitEthernet 0/1)# exit
Device D(config)# router bgp 65535
```

```
Device D(config-router)# neighbor 192.168.4.2 remote-as 65536
Device D(config-router)# neighbor 192.168.5.3 remote-as 65536
Device D(config-router)# network 10.1.1.4 mask 255.255.255.255
```

Configure device RR.

```
Device RR# configure terminal
Device RR(config)# interface loopback 0
Device RR(config-if-Loopback 0)# ip address 10.1.1.5 255.255.255.255
Device RR(config-if-Loopback 0)# exit
Device RR(config)# interface GigabitEthernet 0/1
Device RR(config-if-GigabitEthernet 0/1)# ip address 192.168.1.5 255.255.255.0
Device RR(config-if-GigabitEthernet 0/1)# exit
Device RR(config)# interface GigabitEthernet 0/2
Device RR(config-if-GigabitEthernet 0/2)# ip address 192.168.2.5 255.255.255.0
Device RR(config-if-GigabitEthernet 0/2)# exit
Device RR(config)# interface GigabitEthernet 0/3
Device RR(config-if-GigabitEthernet 0/3)# ip address 192.168.3.5 255.255.255.0
Device RR(config-if-GigabitEthernet 0/3)# exit
Device RR(config)#ip route 192.168.4.0 255.255.255.0 192.168.2.2
Device RR(config)#ip route 192.168.5.0 255.255.255.0 192.168.3.3
Device RR(config)# router bgp 65536
Device RR(config-router)# neighbor 192.168.1.1 remote-as 65536
Device RR(config-router)# neighbor 192.168.1.1 route-reflector-client
Device RR(config-router)# neighbor 192.168.2.2 remote-as 65536
Device RR(config-router)# neighbor 192.168.2.2 route-reflector-client
Device RR(config-router)# neighbor 192.168.3.3 remote-as 65536
```

(2) Configure the ADD-PATH rules for the route reflector RR.

Configure device RR.

```
Device RR# configure terminal
Device RR(config)# router bgp 65536
Device RR(config-router)# bgp additional-paths select best 2
Device RR(config-router)# neighbor 192.168.1.1 advertise additional-paths best 2
Device RR(config-router)# neighbor 192.168.1.1 additional-paths send
```

5. Verification

On device RR, check the BGP neighbor status.

```
Device RR# show ip bgp
BGP table version is 3, local router ID is 10.1.1.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric     LocPrf     Weight Path
* ia10.1.1.4/32    192.168.4.4            0    100      0 65535 i
*>i              192.168.5.4            0    100      0 65535 i
Total number of prefixes 2
```

On device A, run the **show** command to display the BGP neighbor status.

```
Device A# show ip bgp
BGP table version is 2, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric     LocPrf     Weight Path
* i 10.1.1.4/32    192.168.5.4            0    100      0 65535 i
* i              192.168.4.4            0    100      0 65535 i
Total number of prefixes 2
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.168.1.1 255.255.255.0
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.1.5 remote-as 65536
 address-family ipv4
  neighbor 192.168.1.5 activate
  neighbor 192.168.1.5 additional-paths receive
  exit-address-family
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.168.2.2 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 192.168.4.2 255.255.255.0
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
```

```
 neighbor 192.168.2.5 remote-as 65536
 neighbor 192.168.4.4 remote-as 65535
 address-family ipv4
  neighbor 192.168.2.5 activate
  neighbor 192.168.4.4 activate
  exit-address-family
!
```

- Device C configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.168.3.3 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 192.168.5.3 255.255.255.0
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.3.5 remote-as 65536
 neighbor 192.168.5.4 remote-as 65535
 address-family ipv4
  neighbor 192.168.3.5 activate
  neighbor 192.168.5.4 activate
  exit-address-family
!
```

- Device C configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.168.4.4 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 192.168.5.4 255.255.255.0
!
interface Loopback 0
 ip address 10.1.1.4 255.255.255.255
!
router bgp 65535
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
```

```
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.4.2 remote-as 65536
 neighbor 192.168.5.3 remote-as 65536
 address-family ipv4
  network 10.1.1.4 mask 255.255.255.255
  neighbor 192.168.4.2 activate
  neighbor 192.168.5.3 activate
  exit-address-family
!
```

- Device RR configuration file

```
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.168.1.5 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 192.168.2.5 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip address 192.168.3.5 255.255.255.0
!
interface Loopback 0
 ip address 10.1.1.5 255.255.255.255
!
router bgp 65536
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.1.1 remote-as 65536
 neighbor 192.168.2.2 remote-as 65536
 neighbor 192.168.3.3 remote-as 65536
 address-family ipv4
  bgp additional-paths select best 2
  neighbor 192.168.1.1 activate
  neighbor 192.168.1.1 route-reflector-client
  neighbor 192.168.1.1 additional-paths send
  neighbor 192.168.1.1 advertise additional-paths best 2
  neighbor 192.168.2.2 activate
  neighbor 192.168.2.2 route-reflector-client
  neighbor 192.168.3.3 activate
  exit-address-family
!
```

Contents

1 Configuring VRF 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 3
1.2 Restrictions and Guidelines 3
1.3 Configuration Task Summary 3
1.4 Configuring a Single-Protocol VRF 4
1.4.1 Overview 4
1.4.2 Restrictions and Guidelines 4
1.4.3 Configuration Tasks 5
1.4.4 Creating a Single-Protocol VRF 5
1.4.5 Configuring the RD for a Single-Protocol VRF 5
1.4.6 Configuring the RT for a Single-Protocol VRF 6
1.4.7 Configuring the Label Allocation Mode for a Single-Protocol VRF 6
1.4.8 Configuring an Export Policy Associated with a Single-Protocol VRF 7
1.4.9 Configuring an Import Policy Associated with a Single-Protocol VRF 8
1.4.10 Adding an Interface to a Single-Protocol VRF 8
1.4.11 Importing Routes of an Interface to a Single-Protocol VRF 9
1.4.12 Configuring the Maximum Number of Routes for a Single-Protocol VRF 9
1.5 Configuring a Multiprotocol VRF 10
1.5.1 Overview 10

1.5.2 Restrictions and Guidelines 10

1.5.3 Configuration Tasks 10

1.5.4 Creating a Multiprotocol VRF 10

1.5.5 Configuring the Address Family for a Multiprotocol VRF 11

1.5.6 Configuring the RD for a Multiprotocol VRF 11

1.5.7 Configuring the RT for a Multiprotocol VRF 12

1.5.8 Configuring the Label Allocation Mode for a Multiprotocol VRF 13

1.5.9 Configuring an Export Policy Associated with a Multiprotocol VRF 13

1.5.10 Configuring an Import Policy Associated with a Multiprotocol VRF 14

1.5.11 Adding an Interface to a Multiprotocol VRF 15

1.5.12 Importing Routes of an Interface to a Multiprotocol VRF 16

1.5.13 Configuring the Maximum Number of Routes for a Multiprotocol VRF 16

1.6 Configuring a Global VRF 17

1.6.1 Overview 17

1.6.2 Restrictions and Guidelines 17

1.6.3 Configuration Tasks 17

1.6.4 Configuring the Address Family for a Global VRF 17

1.6.5 Configuring the RD for a Global VRF 18

1.6.6 Configuring the RT for a Global VRF 18

1.6.7 Configuring the Label Allocation Mode for a Global VRF 19

1.6.8 Configuring an Export Policy Associated with a Global VRF 20

1.6.9 Configuring an Import Policy Associated with a Global VRF 20

1.6.10 Configuring the Maximum Number of Routes for a Global VRF 21

1.7 Monitoring 21

1.8 Configuration Examples.....22

1.8.1 Enabling Local Inter-VPN Access.....22

1 Configuring VRF

1.1 Introduction

1.1.1 Overview

VPN Routing and Forwarding Table (VRF) is used to resolve local routing conflicts caused by the same IP address space between different Virtual Private Networks (VPNs). One VPN corresponds to one VRF. Each VRF is equivalent to a "virtual router" that receives or advertises VPN routing information. Each VRF includes:

- An independent routing table;
- A set of interfaces belonging to this VRF;
- A set of routing protocols used for this VRF only.

Multiple routing tables on the device that provides the VPN service including a public network routing table and one or more VRFs. The public network routing table is used to forward public network packets, and the VRF is used to forward VPN packets. Routes in the public network routing table are separated from those in VRFs, and routes are separated between VRFs.

Note

- A VPN is a private dedicated network built in the public network. "Virtual" means that the VPN is logically exclusive, but not physically exclusive.
- The private dedicated network is called “private network” for short.

1.1.2 Principles

1. VPN Instance

A VPN instance is used to provide the VPN service. On a device that provides the VPN service, a VPN instance includes the VRFs, interfaces, routing protocol processes, and configurations that belong to the same VPN. Generally, the VRF represents a VPN instance.

2. VPN Route

A VPN route is only used to forward VPN packets. It comes from:

- Direct route and host route generated after an interface is added to the VRF;
- Direct route and host route imported from an interface that is not added to the VRF;
- Static and dynamic routes (RIP, RIPng, OSPFv2, OSPFv3, ISIS, and BGP) in the configured VPN instance.

Note

- For configuration of the static route in a VPN instance, see *Configuring IP Route Basics*.
- For configuration of RIP in a VPN instance, see *Configuring RIP*.
- For configuration of RIPng in a VPN instance, see *Configuring RIPng*.
- For configuration of OSPFv2 in a VPN instance, see *Configuring OSPFv2*.
- For configuration of OSPFv3 in a VPN instance, see *Configuring OSPFv3.*

- For configuration of ISIS in a VPN instance, see *Configuring ISIS*.
- For configuration of BGP in a VPN instance, see *Configuring BGP*.

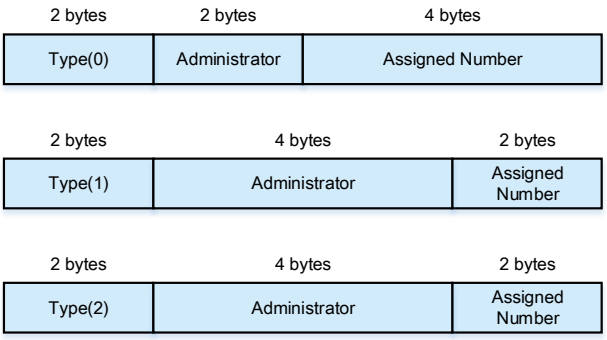
3. VPN Route Attribute

A VPN route has two attributes: Route Distinguisher (RD) and Route Target (RT).

- The RD is used to resolve routing conflicts when the Border Gateway Protocol (BGP) advertises routes. If different VPNs have the same network addresses, the BGP only selects an optimum route from these addresses and advertises this route. As a result, some VPNs cannot receive the routing information. To resolve this problem, you can add different RDs to the same addresses. Based on the different RDs carried in VPN information, the BGP can distinguish the same network addresses, and therefore each VPN can receive its own routing information.

  Generally, a unique RD value is specified for each VPN. A VPN route carries only one RD value. An RD consists of a **Type** field, an **Administrator** field, and an **Assigned Number** field. As shown in Figure 1-1, based on the value of the **Type** field, the RD is encoded in three formats:

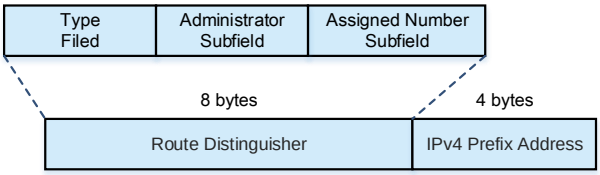
Figure 1-1 RD structure



  - When **Type** is set to **0**, the **Administrator** field has two bytes and is set to an Autonomous System (AS) number, which must be a public AS number; the **Assigned Number** field has four bytes and is managed by the service provider (SP).
  - When **Type** is set to **1**, the **Administrator** field has four bytes and is set to an IPv4, which must be a global IP address; the **Assigned Number** field has two bytes and is managed by the SP.
  - When **Type** is set to **2**, the **Administrator** field has four bytes and is set to a 4-byte AS number; the **Assigned Number** field has two bytes and is managed by the SP.

  An IPv4 address with the RD is called VPN-IPv4 address, as shown in Figure 1-2. After receiving an IPv4 route, the BGP converts it into a globally unique VPN-IPv4 route, and advertises this route in the public network.

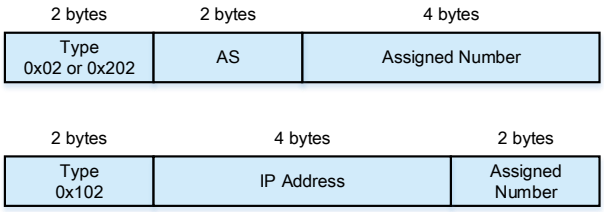
Figure 1-2 VPN-IPv4 address structure



- RT is used to control the advertising and installation policies of VPN routes. The RT attribute falls into the following two types:
  - **Import**: When a device receives the advertised VPN-IPv4 route, the device checks the **Export** attribute of this route. If the **Import** attribute of a specified VPN instance on the device matches the **Export** attribute, the device adds the route to the VPN instance.
  - **Export**: After the local device learns an IPv4 route, it converts this route into a VPN-IPv4 route. The **Export** attribute is set for this route and advertised as the BGP extended community attribute to other devices together with the route.

  The BGP extended community attribute defines the RT structure, as shown in Figure 1-3.

Figure 1-3 RT structure



The RT value and the RD value are similarly defined. When **Type** is set to **0x02** or **0x202**, the AS number must be public. When **Type** is set to **0x102**, the IPv4 address must be a global IP address.

1.1.3 Protocols and Standards

- RFC4364: BGP/MPLS IP Virtual Private Networks (VPNs)

1.2 Restrictions and Guidelines

- You can configure only one type of VRF: single-protocol VRF or multiprotocol VRF.
- Single-protocol VRFs only support IPv4, whereas multiprotocol VRFs support both IPv4 and IPv6.

1.3 Configuration Task Summary

The configuration tasks below are mutually exclusive. Please configure only one task.

- Configuring a Single-Protocol VRF
  a. Creating a Single-Protocol VRF
  b. (Optional) Configuring the RD for a Single-Protocol VRF
  c. (Optional) Configuring the RT for a Single-Protocol VRF

d. (Optional) Configuring the Label Allocation Mode for a Single-Protocol VRF

e. (Optional) Configuring an Export Policy Associated with a Single-Protocol VRF

f. (Optional) Configuring an Import Policy Associated with a Single-Protocol VRF

g. Adding an Interface to a Single-Protocol VRF

h. (Optional) Importing Routes of an Interface to a Single-Protocol VRF

i. (Optional) Configuring the Maximum Number of Routes for a Single-Protocol VRF

- Configuring a Multiprotocol VRF

a. Creating a Multiprotocol VRF

b. (Optional) Configuring the Address Family for a Multiprotocol VRF

c. (Optional) Configuring the RD for a Multiprotocol VRF

d. (Optional) Configuring the RT for a Multiprotocol VRF

e. (Optional) Configuring the Label Allocation Mode for a Multiprotocol VRF

f. (Optional) Configuring an Export Policy Associated with a Multiprotocol VRF

g. (Optional) Configuring an Import Policy Associated with a Multiprotocol VRF

h. Adding an Interface to a Multiprotocol VRF

i. (Optional) Importing Routes of an Interface to a Multiprotocol VRF

j. (Optional)Configuring the Maximum Number of Routes for a Multiprotocol VRF

- Configuring a Global VRF

a. Configuring the Address Family for a Global VRF

b. (Optional) Configuring the RD for a Global VRF

c. (Optional) Configuring the RT for a Global VRF

d. (Optional) Configuring the Label Allocation Mode for a Global VRF

e. (Optional) Configuring an Export Policy Associated with a Global VRF

f. (Optional) Configuring an Import Policy Associated with a Global VRF

g. (Optional) Configuring the Maximum Number of Routes for a Global VRF

1.4 Configuring a Single-Protocol VRF

1.4.1 Overview

A single-protocol VRF is configured to manage VPN routes.

1.4.2 Restrictions and Guidelines

- If a device forwards only packets of a specified VPN or only public network packets, you do not need to configure a single-protocol VRF.
- If the device needs to forward both the public network packets and VPN packets or forward packets from multiple VPNs, VRFs must be created to separate routes.
- You need to add static or dynamic routes (RIP, OSPF, ISIS, and BGP) to a VRF.
- Only IPv4 is supported.

1.4.3 Configuration Tasks

The configuration of a single-protocol VRF includes the following tasks:

(1) Creating a Single-Protocol VRF

(2) (Optional) Configuring the RD for a Single-Protocol VRF

(3) (Optional) Configuring the RT for a Single-Protocol VRF

(4) (Optional) Configuring the Label Allocation Mode for a Single-Protocol VRF

(5) (Optional) Configuring an Export Policy Associated with a Single-Protocol VRF

(6) (Optional) Configuring an Import Policy Associated with a Single-Protocol VRF

(7) Adding an Interface to a Single-Protocol VRF

(8) (Optional) Importing Routes of an Interface to a Single-Protocol VRF

(9) (Optional) Configuring the Maximum Number of Routes of a Single-Protocol VRF

1.4.4 Creating a Single-Protocol VRF

1. Overview

This section describes how to create a single-protocol VRF for each VPN.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a single-protocol VRF, and enter the VRF configuration mode.

ip vrf *vrf-name*

No single-protocol VRF is configured by default.

(4) (Optional) Configure the description for a single-protocol VRF.

description *description*

No description is configured by default.

1.4.5 Configuring the RD for a Single-Protocol VRF

1. Overview

This section describes how to configure the RD to resolve routing conflicts when the BGP advertises routes.

2. Restrictions and Guidelines

- Configure the RD command in single-protocol VRF configuration mode.
- If you have configured a VRF value and its RD value and want to modify the RD value, you must first delete the VRF, reconfigure the VRF, and then configure the RD value.
- You can configure only one RD value for a VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the single-protocol VRF configuration mode.

ip vrf *vrf-name*

(4) Configure the RD.

rd *rd-value*

No RD value is configured by default.

1.4.6 Configuring the RT for a Single-Protocol VRF

1. Overview

This section describes how to configure the RT value to control advertisement of VPN routes.

2. Restrictions and Guidelines

- Configure the RT value in single-protocol VRF configuration mode.
- You can configure multiple **Import** or **Export** values for each VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the single-protocol VRF configuration mode.

ip vrf *vrf-name*

(4) Configure the RT.

route-target { **both** | **export** | **import** } *route-value*

No RT is configured by default.

1.4.7 Configuring the Label Allocation Mode for a Single-Protocol VRF

1. Overview

This section describes how to configure the label allocation mode for a single-protocol VRF.

2. Restrictions and Guidelines

- Route-based label allocation mode: One route corresponds to one label. The advantage is that the system can look up the ILM table based on the label value and quickly forward packets to the next hop. The disadvantage is that the capacity of the ILM table must be large.
- VRF-based label allocation mode: One VRF corresponds to one label. The advantage is that all routes in the VRF share this label, which reduces the capacity of the ILM table. The disadvantage is that packet

forwarding is slower than that in route-based label allocation mode. This is because the system needs to look up the table twice in the forwarding process. It first looks up the ILM table to find the VRF where the packet is located, and then forwards the packet based on the destination IP address in the routing table of the VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the single-protocol VRF configuration mode.

ip vrf *vrf-name*

(4) Configure the label allocation mode.

alloc-label { **per-route** | **per-vrf** }

No label allocation mode is configured by default.

1.4.8 Configuring an Export Policy Associated with a Single-Protocol VRF

1. Overview

This section describes how to configure a policy for exporting the extended community attributes of VPN routes from the local VRF to a remote device.

2. Restrictions and Guidelines

- To more precisely control the extended community attributes of exported routes, you can define a precise rule as needed in the associated route map.
- You can run this command to add or modify the extended community attributes defined by the **route-target export** command.
- You can only run the **match ip address** and **set extcommunity** commands to configure rules for a route map associated by this command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the single-protocol VRF configuration mode.

ip vrf *vrf-name*

(4) Configure the associated export policy.

export map *route-map-name*

No export policy associated with the VRF is configured by default.

1.4.9 Configuring an Import Policy Associated with a Single-Protocol VRF

1. Overview

This section describes how to configure a policy for importing VPN routes from a remote device to the local VRF.

2. Restrictions and Guidelines

- To more precisely filter routes imported to the local VRF, you can define a precise rule as needed in the associated route map.
- The rule defined by the **import map** command takes effect after the **Import** extended community attributes defined in the VRF. That is, only after the route matches the extended community attributes defined by the **route-target import** command in the VRF, can the VPN routes received from the remote device be filtered again by rules defined by the **import map** command.
- You can only run the **match ip address** and **match extcommunity** commands to configure rules for a route map associated by the **import map** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the single-protocol VRF configuration mode.

ip vrf *vrf-name*

(4) Configure the associated import policy.

import map *route-map-name*

No import policy associated with the VRF is configured by default.

1.4.10 Adding an Interface to a Single-Protocol VRF

1. Overview

This section describes how to add an interface to a specified VRF. This VRF is used to forward incoming packets of the interface.

2. Restrictions and Guidelines

You must add the interface to the single-protocol VRF before configuring the IPv4 address. If you configure the IPv4 address for an interface and then add the interface to the single-protocol VRF, the configuration of the IPv4 address fails, but the configuration of the IPv6 address is retained.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Add the interface to the single-protocol VRF.

ip vrf forwarding *vrf-name*

By default, an interface does not belong to any VRF.

1.4.11 Importing Routes of an Interface to a Single-Protocol VRF

1. Overview

This section describes how to import the host route and direct route of an interface to a specified VRF.

2. Restrictions and Guidelines

- If you need to use policy-based routing (PBR) to select the VRF, configure the **ip vrf receive** command on the interface to which PBR is applied, and import the direct route and host route on the interface to each VRF available for choice.
- If you need to import the host route and direct route of an interface to multiple VRFs, run this command multiple times.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Import the host route and direct route of the interface to a specified VRF.

ip vrf receive *vrf-name*

The direct route and host route of an interface are not imported to any specified VRF by default.

The **ip vrf forwarding** and **ip vrf receive** commands are mutually exclusive on a specified interface. Unlike the **ip vrf forwarding** command, the **ip vrf receive** command does not add the interface to the VRF, and the interface does not belong to any VRF.

1.4.12 Configuring the Maximum Number of Routes for a Single-Protocol VRF

1. Overview

This section describes how to configure the maximum number of routes for a single-protocol VRF.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the single-protocol VRF configuration mode.

ip vrf *vrf-name*

(4) Enter the single-protocol VRF address family configuration mode.

address-family { **ipv4** | **ipv6** }

(5) Configure the maximum number of routes for a single-protocol VRF.

maximum routes *limit* { **warning-only** | *warning-threshold* }

No maximum number of routes is configured by default.

1.5 Configuring a Multiprotocol VRF

1.5.1 Overview

This section describes how to configure a multiprotocol VRF to manage VPN routes. You can configure the address family to support IPv4 and IPv6. The BGP helps you to flexibly isolate VPNs or allow inter-VPN access, or provide the VPN service in an IP/MPLS backbone network.

1.5.2 Restrictions and Guidelines

- If a device forwards only packets of a specified VPN or only public network packets, you do not need to configure a multiprotocol VRF.
- If the device needs to forward both the public network packets and VPN packets or forward packets from multiple VPNs, VRFs must be created to separate routes.
- You need to add static or dynamic routes (RIP, OSPF, ISIS, and BGP) to a VRF.

1.5.3 Configuration Tasks

The configuration of a multiprotocol VRF includes the following tasks:

(1) Creating a Multiprotocol VRF

(2) Configuring the Address Family for a Multiprotocol VRF

(3) (Optional) Configuring the RD for a Multiprotocol VRF

(4) (Optional) Configuring the RT for a Multiprotocol VRF

(5) (Optional) Configuring the Label Allocation Mode for a Multiprotocol VRF

(6) (Optional) Configuring an Export Policy Associated with a Multiprotocol VRF

(7) (Optional) Configuring an Import Policy Associated with a Multiprotocol VRF

(8) Adding an Interface to a Multiprotocol VRF

(9) (Optional) Importing Routes of an Interface to a Multiprotocol VRF

(10) (Optional) Configuring the Maximum Number of Routes for a Multiprotocol VRF

1.5.4 Creating a Multiprotocol VRF

1. Overview

This section describes how to create a multiprotocol VRF for each VPN.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a multiprotocol VRF, and enter the multiprotocol VRF configuration mode.

vrf definition *vrf-name*

No multiprotocol VRF exists by default.

(4) (Optional) Configure the description for a multiprotocol VRF.

description *description*

No description is configured by default.

1.5.5 Configuring the Address Family for a Multiprotocol VRF

1. Overview

This section describes how to enable the IPv4/IPv6 address family for a multiprotocol VRF, and enter the configuration mode.

2. Restrictions and Guidelines

You can configure the address family for each created VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the multiprotocol VRF configuration mode.

vrf definition *vrf-name*

(4) Configure the address family. Configure at least one of the following tasks.

- Configure the IPv4 address family, and enter the VRF IPv4 address family submode.

  address-family ipv4

- Configure the IPv6 address family, and enter the VRF IPv6 address family submode.

  address-family ipv6

No address family is configured for a multiprotocol VRF by default.

1.5.6 Configuring the RD for a Multiprotocol VRF

1. Overview

This section describes how to configure the RD to resolve routing conflicts when the BGP advertises routes.

2. Restrictions and Guidelines

- Configure the RD command in multiprotocol VRF configuration mode.
- If you have configured a VRF value and its RD value and want to modify the RD value, you must first delete the VRF, reconfigure the VRF, and then configure the RD value.
- You can configure only one RD value for a VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the multiprotocol VRF configuration mode.

vrf definition *vrf-name*

(4) Configure the RD.

rd *rd-value*

No RD value is configured by default.

1.5.7 Configuring the RT for a Multiprotocol VRF

1. Overview

This section describes how to configure the RT group to control advertisement of VPN routes.

2. Restrictions and Guidelines

- Configure the RT value in multiprotocol VRF mode or multiprotocol VRF address family mode.
- You can configure multiple **Import** or **Export** values for each VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the multiprotocol VRF configuration mode.

vrf definition *vrf-name*

(4) Configure the RT. Configure one of the following tasks.

- In multiprotocol VRF configuration mode, run the following command to configure the RT:

  route-target { **both** | **export** | **import** } *route-value*

- In multiprotocol VRF address family configuration mode, run the following command to configure the RT:

  address-family { **ipv4** | **ipv6** }

  No IPv4 or IPv6 protocol is enabled for the multiprotocol VRF by default.

  route-target { **both** | **export** | **import** } *route-value*

No RT is configured by default.

1.5.8 Configuring the Label Allocation Mode for a Multiprotocol VRF

1. Overview

This section describes how to configure the label allocation mode for a multiprotocol VRF.

2. Restrictions and Guidelines

- Route-based label allocation mode: One route corresponds to one label. The advantage is that the system can look up the ILM table based on the label value and quickly forward packets to the next hop. The disadvantage is that the capacity of the ILM table must be large.
- VRF-based label allocation mode: One VRF corresponds to one label. The advantage is that all routes in the VRF share this label, which reduces the capacity of the ILM table. The disadvantage is that packet forwarding is slower than that in route-based label allocation mode. This is because the system needs to look up the table twice in the forwarding process. It first looks up the ILM table to find the VRF where the packet is located, and then forwards the packet based on the destination IP address in the routing table of the VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the multiprotocol VRF configuration mode.

vrf definition *vrf-name*

(4) Enter the address family configuration mode. Configure at least one of the following tasks.

- Enter the IPv4 address family configuration mode.

  address-family ipv4

- Enter the IPv6 address family configuration mode.

  address-family ipv6

A multiprotocol VRF does not enter any address family configuration mode by default.

(5) Configure the label allocation mode.

alloc-label { **per-route** | **per-vrf** }

No label allocation mode is configured by default.

1.5.9 Configuring an Export Policy Associated with a Multiprotocol VRF

1. Overview

This section describes how to configure a policy for exporting the extended community attributes of VPN routes from the local VRF to the remote device

2. Restrictions and Guidelines

- To more precisely control the extended community attributes of exported routes, you can define a precise

rule as needed in the associated route map.

- You can run this command to add or modify the extended community attributes defined by the **route-target export** command.
- You can only run the **match ip address** and **set extcommunity** commands to configure rules for a route map associated by this command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the multiprotocol VRF configuration mode.

vrf definition *vrf-name*

(4) Enter the address family configuration mode. Configure at least one of the following tasks.

- Enter the IPv4 address family configuration mode.

  address-family ipv4

- Enter the IPv6 address family configuration mode.

  address-family ipv6

A multiprotocol VRF does not enter any address family configuration mode by default.

(5) Configure the associated export policy.

export map *route-map-name*

No export policy associated with the VRF is configured by default.

1.5.10 Configuring an Import Policy Associated with a Multiprotocol VRF

1. Overview

This section describes how to configure a policy for importing VPN routes from a remote device to the local VRF.

2. Restrictions and Guidelines

- To more precisely filter routes imported to the local VRF, you can define a precise rule as needed in the associated route map.
- The rule defined by the **import map** command takes effect after the **Import** extended community attributes defined in the VRF. That is, only after these routes match the extended community attributes defined by the **route-target import** command in the VRF, can the VPN routes received from the remote device be filtered again by rules defined the **import map** command.
- You can only run the **match ip address** and **match extcommunity** commands to configure rules for a route map associated by the import map command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the multiprotocol VRF configuration mode.

vrf definition *vrf-name*

(4) Enter the address family configuration mode. Configure at least one of the following tasks.

- Enter the IPv4 address family configuration mode.

  address-family ipv4

- Enter the IPv6 address family configuration mode.

  address-family ipv6

A multiprotocol VRF does not enter any address family configuration mode by default.

(5) Configure the associated import policy.

import map *route-map-name*

No import policy associated with the VRF is configured by default.

1.5.11 Adding an Interface to a Multiprotocol VRF

1. Overview

This section describes how to add an interface to a specified VRF. This VRF is used to forward incoming packets of the interface.

2. Restrictions and Guidelines

- After this command is executed, the direct route and host route on the interface are automatically imported to the VRF.
- Before you add an interface to a multiprotocol VRF, enable the address family for the table. If the IPv4 address family is disabled when you add an interface to a multiprotocol VRF, you are not allowed to configure the IPv4 and VRRP IPv4 addresses on this interface. If the IPv6 address family is disabled when you add an interface to a multiprotocol VRF, you are not allowed to configure the IPv6 and VRRP IPv6 addresses on this interface.
- You must add an interface to the multiprotocol VRF before configuring the IPv4/IPv6 or VRRP IPv4/IPv6 addresses on the interface. When you add an interface to a multiprotocol VRF, existing IPv4/IPv6 or VRRP IPv4/IPv6 addresses on the interface are deleted, and the IPv6 protocol is disabled on the interface.
- If the IPv4 address family is deleted from the multiprotocol VRF, the IPv4 and VRRP IPv4 addresses of all interfaces added to this VRF are deleted, and the IPv4 static routes in the VRF or the IPv4 static routes with this VRF as their next-hop VRF are also deleted.
- If the IPv6 address family is deleted from the multiprotocol VRF, the IPv6 and VRRP IPv6 addresses of all interfaces added to the VRF are deleted, the IPv6 protocol is disabled on the interface, and the IPv6 static routes in the VRF or the IPv6 static routes with this VRF as their next-hop VRF are also deleted.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Add the interface to the multiprotocol VRF.

vrf forwarding *vrf-name*

By default, an interface does not belong to any VRF.

1.5.12 Importing Routes of an Interface to a Multiprotocol VRF

1. Overview

This section describes how to import the host route and direct route of an interface to a specified VRF.

2. Restrictions and Guidelines

- If you need to use PBR to select the VRF, configure the **vrf receive** command on the interface to which PBR is applied to import the direct route and host route on the interface to each VRF available for choice.
- If you need to import the host route and direct route of an interface to multiple VRFs, run this command multiple times.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Import the host route and direct route of the interface to a specified VRF.

vrf receive *vrf-name*

The **vrf forwarding** and **vrf receive** commands are mutually exclusive on a specified interface. Unlike the **vrf forwarding** command, the **vrf receive** command does not add an interface to the specified VRF, and the interface does not belong to any VRF.

1.5.13 Configuring the Maximum Number of Routes for a Multiprotocol VRF

1. Overview

This section describes how to configure the maximum number of routes for a multiprotocol VRF.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the multiprotocol VRF configuration mode.

vrf definition *vrf-name*

(4) Enter the multiprotocol VRF address family configuration mode.

address-family { **ipv4** | **ipv6** }

(5) Configure the maximum number of routes for a multiprotocol VRF.

maximum routes *limit* { **warning-only** | *warning-threshold* }

No maximum number of routes is configured by default.

1.6 Configuring a Global VRF

1.6.1 Overview

A global VRF is configured to manage VPN routes. The global VRF is created by default.

1.6.2 Restrictions and Guidelines

- If a device forwards only packets of a specified VPN or only public network packets, you do not need to configure a VRF.
- If the device needs to forward both the public network packets and VPN packets or forward packets from multiple VPNs, VRFs must be created to separate routes.
- You need to add static or dynamic routes (RIP, OSPF, ISIS, and BGP) to a VRF.

1.6.3 Configuration Tasks

The configuration of a global VRF includes the following tasks:

(1) Configuring the Address Family for a Global VRF

(2) (Optional) Configuring the RD for a Global VRF

(3) (Optional) Configuring the RT for a Global VRF

(4) (Optional) Configuring the Label Allocation Mode for a Global VRF

(5) (Optional) Configuring an Export Policy Associated with a Global VRF

(6) (Optional) Configuring an Import Policy Associated with a Global VRF

(7) (Optional) Configuring the Maximum Number of Routes for a Global VRF

1.6.4 Configuring the Address Family for a Global VRF

1. Overview

This section describes how to enable the IPv4/IPv6 address family for a global VRF, and enter the configuration mode.

2. Restrictions and Guidelines

You can configure the address family for each created VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the global VRF configuration mode.

vrf global-vrf

(4) (Optional) Configure description for the global VRF.

description *description*

No description is configured by default.

(5) Configure the address family. Configure at least one of the following tasks.

- Configure the IPv4 address family, and enter the VRF IPv4 address family submode.

  address-family ipv4

- Configure the IPv6 address family, and enter the VRF IPv6 address family submode.

  address-family ipv6

IPv4/IPv6 address family is enabled by default.

1.6.5 Configuring the RD for a Global VRF

1. Overview

This section describes how to configure the RD to resolve routing conflicts when the BGP advertises routes.

2. Restrictions and Guidelines

- Configure the RD command in global VRF configuration mode.
- If you have configured a VRF value and its RD value and want to modify the RD value, you must first delete the VRF, reconfigure the VRF, and then configure the RD value.
- You can configure only one RD value for a VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the global VRF configuration mode.

vrf global-vrf

(4) Configure the RD.

rd *rd-value*

No RD value is configured by default.

1.6.6 Configuring the RT for a Global VRF

1. Overview

This section describes how to configure the RT value to control advertisement of VPN routes.

2. Restrictions and Guidelines

- Configure the RT value in global VRF configuration mode or global VRF address family configuration mode.
- You can configure multiple **Import** or **Export** values for each VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the global VRF configuration mode.

vrf global-vrf

(4) (Optional) Enter the global VRF address family configuration mode.

address-family { **ipv4** | **ipv6** }

(5) Configure the RT.

route-target { **both** | **export** | **import** } *route-value*

No RT is configured by default.

1.6.7 Configuring the Label Allocation Mode for a Global VRF

1. Overview

This section describes how to configure the label allocation mode for a global VRF.

2. Restrictions and Guidelines

- Route-based label allocation mode: One route corresponds to one label. The advantage is that the system can look up the ILM table based on the label value and quickly forward packets to the next hop. The disadvantage is that the capacity of the ILM table must be large.
- VRF-based label allocation mode: One VRF corresponds to one label. The advantage is that all routes in the VRF share this label, which reduces the capacity of the ILM table. The disadvantage is that packet forwarding is slower than that in route-based label allocation mode. This is because the system needs to look up the table twice in the forwarding process. It first looks up the ILM table to find the VRF where the packet is located, and then forwards the packet based on the destination IP address in the routing table of the VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the global VRF configuration mode.

vrf global-vrf

(4) (Optional) Enter the global VRF address family configuration mode.

address-family { **ipv4** | **ipv6** }

(5) Configure the label allocation mode.

alloc-label { **per-route** | **per-vrf** }

No label allocation mode is configured by default.

1.6.8 Configuring an Export Policy Associated with a Global VRF

1. Overview

This section describes how to configure a policy for exporting the extended community attributes of VPN routes from the local VRF to a remote device.

2. Restrictions and Guidelines

- To more precisely control the extended community attributes of exported routes, you can define a precise rule as needed in the associated route map.
- You can run this command to add or modify the extended community attributes defined by the **route-target export** command.
- You can only run the **match ip address** and **set extcommunity** commands to configure rules for a route map associated by this command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the global VRF configuration mode.

vrf global-vrf

(4) Enter the global VRF address family configuration mode.

address-family { **ipv4** | **ipv6** }

(5) Configure the associated export policy.

export map *route-map-name*

No export policy associated with the VRF is configured by default.

1.6.9 Configuring an Import Policy Associated with a Global VRF

1. Overview

This section describes how to configure a policy for importing VPN routes from a remote device to the local VRF.

2. Restrictions and Guidelines

- To more precisely filter routes imported to the local VRF, you can define a precise rule as needed in the associated route map.
- The rule defined by the **import map** command takes effect after the **Import** extended community attributes defined in the VRF. That is, only after the route matches the extended community attributes defined by the

route-target import command in the VRF, can the VPN routes received from the remote device be filtered again by rules defined by the **import map** command.

- You can only run the **match ip address** and **match extcommunity** commands to configure rules for a route map associated by the **import map** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the global VRF configuration mode.

vrf global-vrf

(4) Enter the global VRF address family configuration mode.

address-family { **ipv4** | **ipv6** }

(5) Configure the associated import policy.

import map *route-map-name*

No import policy associated with the VRF is configured by default.

1.6.10 Configuring the Maximum Number of Routes for a Global VRF

1. Overview

This section describes how to configure the maximum number of routes for a global VRF.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the global VRF configuration mode.

vrf global-vrf

(4) Enter the global VRF address family configuration mode.

address-family { **ipv4** | **ipv6** }

(5) Configure the maximum number of routes for a global VRF.

maximum routes *limit* { **warning-only** | *warning-threshold* }

No maximum number of routes is configured by default.

1.7 Monitoring

Run the **show** command to check the running status of a configured function and verify the configuration effect.

Run the **clear** commands to clear information.

Caution

Running the **clear** commands may interrupt services due to loss of vital information.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 VRF Monitoring

Command	Purpose
show ip vrf [**brief | count | detail | interfaces**] [*vrf-name*]	Displays a single-protocol VRF.
show global-vrf [**count** | **brief** | **detail** | **ipv4** | **ipv6**]	Displays a global VRF.
show vrf [**brief | count | detail | ipv4 | ipv6**] [*vrf-name*]	Displays a multiprotocol VRF.
clear ip mroute [**vrf** *vid*] **statistics** { * | *group-address* [*source-address*] }	Clears the multicast route statistics.
clear ip pim dense-mode [**vrf** *vid*] **track**	Clears the PIM-DM packet statistics.
clear ip route vrf *vrf-name*	Clears the routes in a specified VRF.
debug vrf	Displays the debugging information when a VRF is created, an address family is enabled, and an interface is added to the VRF.
debug vrf interface	Displays the debugging information of interface-related VRF operations.

1.8 Configuration Examples

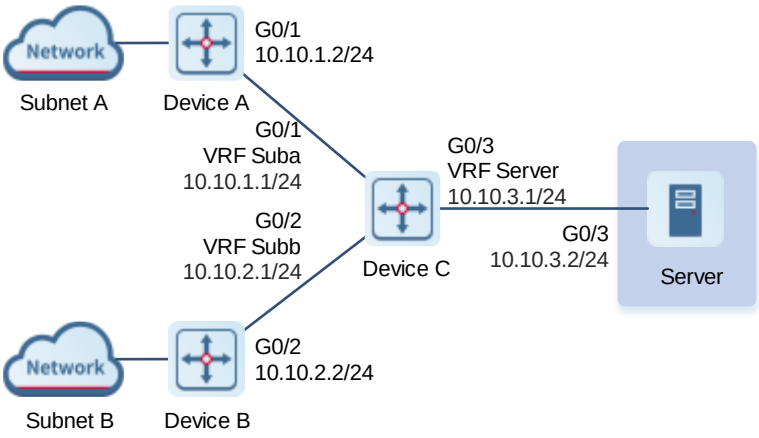
1.8.1 Enabling Local Inter-VPN Access

1. Requirements

Subnet A, Subnet B, and Server are three VPNs that have separate address spaces. Subnet A runs RIP, Subnet B runs OSPF, and Servers is a network segment directly connected to Device C. Routes in Subnet A are separated from those in Subnet B, but both Subnet A and Subnet B can access Server.

2. Topology

Figure 1-4 Local inter-VPN access



3. Notes

- On Device C, create a VRF named **Suba**, add the interface directly connected to Device A to the VRF **Suba**. Associate the VRF **Suba** of Device C with Device A by using RIP.
- On Device C, create a VRF named **Subb**, add the interface directly connected to Device B to the VRF **Subb**. Associate the VRF **Subb** of Device C with Device B by using OSPF.
- On Device C, create a VRF named **Server**, add the interface directly connected to Server to the VRF **Server**.
- On Device C, configure RTs for three VRFs, including **Suba**, **Subb**, and **Server**. Import the routes of **Suba** and **Subb** to **Server**, and the routes of **Server** to **Suba** and **Subb**.
- On Device C, configure the BGP, and import the RIP routes to the IPv4 VRF **Suba**, the OSPF routes to the IPv4 VRF **Subb**, and the direct routes to the IPv4 VRF **Server**.

4. Procedure

(1) (Omitted) Configure the IP address for the device.

(2) Create VRFs on Device C.

Create a VRF named **Suba**, add the interface G0/1 directly connected to Device A to the VRF **Suba**.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# ip vrf Suba
DeviceC(config-vrf)# rd 100:1
DeviceC(config-vrf)# route-target import 100:3
DeviceC(config-vrf)# route-target export 100:1
DeviceC(config-vrf)# exit
DeviceC(config)# interface gigabitethernet 0/1
DeviceC(config-GigabitEthernet 0/1)# ip vrf forwarding Suba
DeviceC(config-GigabitEthernet 0/1)# ip address 10.10.1.1 255.255.255.0
DeviceC(config-GigabitEthernet 0/1)# exit
```

Create a VRF named **Subb**, add the interface G0/2 directly connected to Device B to the VRF **Subb**.

```
DeviceC(config)# ip vrf Subb
DeviceC(config-vrf)# rd 100:2
DeviceC(config-vrf)# route-target import 100:3
DeviceC(config-vrf)# route-target export 100:2
DeviceC(config-vrf)# exit
DeviceC(config)# interface gigabitethernet 0/2
DeviceC(config-GigabitEthernet 0/2)# ip vrf forwarding Subb
DeviceC(config-GigabitEthernet 0/2)# ip address 10.10.2.1 255.255.255.0
DeviceC(config-GigabitEthernet 0/2)# exit
```

Create a VRF named **Server**, add the interface G0/3 directly connected to Server to the VRF **Server**.

```
DeviceC(config)# ip vrf Server
DeviceC(config-vrf)# rd 100:3
DeviceC(config-vrf)# route-target import 100:1
DeviceC(config-vrf)# route-target import 100:2
DeviceC(config-vrf)# route-target export 100:3
DeviceC(config-vrf)# exit
DeviceC(config)# interface gigabitethernet 0/3
DeviceC(config-GigabitEthernet 0/3)# ip vrf forwarding Server
DeviceC(config-GigabitEthernet 0/3)# ip address 10.10.3.1 255.255.255.0
DeviceC(config-GigabitEthernet 0/3)# exit
```

(3) Enable the routing protocol.

Enable the routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# router rip
DeviceA(config-router)# version 2
DeviceA(config-router)# no auto-summary
DeviceA(config-router)# network 10.10.1.0 0.0.0.255
```

Enable the routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# router ospf 1
DeviceB(config-router)# network 10.10.2.0 0.0.0.255 area 0
```

Enable the routing protocol on Device C.

```
DeviceC(config)# router rip
DeviceC(config-router)# address-family ipv4 vrf Suba
DeviceC(config-router-af)# version 2
DeviceC(config-router-af)# no auto-summary
DeviceC(config-router-af)# network 10.10.1.0 0.0.0.255
DeviceC(config-router-af)# exit-address-family
DeviceC(config-router)# exit
DeviceC(config)# router ospf 2 vrf Subb
DeviceC(config-router)# network 10.10.2.0 0.0.0.255 area 0
```

```
DeviceC(config-router)# exit
```

(4) Import routes to VRFs.

Import routes to VRFs on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# router bgp 200
DeviceC(config-router)# address-family ipv4 vrf Suba
DeviceC(config-router-af)# redistribute rip
DeviceC(config-router-af)# exit-address-family
DeviceC(config-router)# address-family ipv4 vrf Subb
DeviceC(config-router-af)# redistribute ospf 2
DeviceC(config-router-af)# exit-address-family
DeviceC(config-router)# address-family ipv4 vrf Server
DeviceC(config-router-af)# redistribute connected
DeviceC(config-router-af)# exit-address-family
DeviceC(config-router)# exit
```

5. Verification

Verify the information of interfaces added to VRFs on Device C.

```
DeviceC> enable
DeviceC# show ip vrf interfaces
Interface           IP-Address  VRF     Protocol
GigabitEthernet 0/1   10.10.1.1   Suba    up
GigabitEthernet 0/2   10.10.2.1   Subb    up
GigabitEthernet 0/3   10.10.3.1   Server   up
```

Verify that the routes in **Suba** are separated from those in **Subb**, and routes of **Server** are shared on Device C.

```
DeviceC# show ip route vrf Suba
Routing Table: Suba

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C   10.10.1.0/24 is directly connected, GigabitEthernet 0/1
C   10.10.1.1/32 is local host.
B   10.10.3.0/24 [20/0] via 0.0.0.0, 00:01:21, GigabitEthernet 0/3

DeviceC# show ip route vrf Subb
Routing Table: Subb

Codes:  C - connected, S - static, R - RIP, B - BGP
```

```
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C   10.10.2.0/24 is directly connected, GigabitEthernet 0/2
C   10.10.2.1/32 is local host.
B   10.10.3.0/24 [20/0] via 0.0.0.0, 00:04:03, GigabitEthernet 0/3

DeviceC# show ip route vrf Server
Routing Table: Server

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
B   10.10.1.0/24 [20/1] via 0.0.0.0, 03:00:15, GigabitEthernet 0/1
B   10.10.2.0/24 [20/1] via 0.0.0.0, 00:00:14, GigabitEthernet 0/2
C   10.10.3.0/24 is directly connected, GigabitEthernet 0/3
C   10.10.3.1/32 is local host.
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.10.1.2 255.255.255.0
!
router rip
 version 2
 network 10.10.1.0 0.0.0.255
 no auto-summary
!
```

Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/2
 no switchport
```

```
 ip address 10.10.2.2 255.255.255.0
!
router ospf 2
 network 10.10.2.0 0.0.0.255 area 0
!
```

Device C configuration file

```
hostname DeviceC
!
ip vrf Server
 rd 100:3
 route-target export 100:3
 route-target import 100:2
 route-target import 100:1
!
ip vrf Suba
 rd 100:1
 route-target export 100:1
 route-target import 100:3
!
ip vrf Subb
 rd 100:2
 route-target export 100:2
 route-target import 100:3
!
interface GigabitEthernet 0/1
 no switchport
 ip vrf forwarding Suba
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip vrf forwarding Subb
 ip address 10.10.2.1 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip vrf forwarding Server
 ip address 10.10.3.1 255.255.255.0
!
router bgp 200
 address-family ipv4 vrf Suba
  redistribute rip
  exit-address-family
 !
 address-family ipv4 vrf Subb
  redistribute ospf 2 match internal
```

```
  exit-address-family
 !
 address-family ipv4 vrf Server
  redistribute connected
  exit-address-family
!
router ospf 2 vrf Subb
 network 10.10.2.0 0.0.0.255 area 0
!
router rip
 address-family ipv4 vrf Suba
  version 2
  network 10.10.1.0 0.0.0.255
  no auto-summary
  exit-address-family
!
```

Server configuration file

```
hostname Server
!
interface GigabitEthernet 0/3
 no switchport
 ip address 10.10.3.2 255.255.255.0
!
```

7. Common Errors

- An interface is added to a VRF after the IP address of the interface is configured. In this case, the IP address of the interface is deleted.
- When a physical link is shared by multiple VPNs, the physical interface is added to a VRF.
- VPN routes are not introduced to BGP.

Contents

1 Configuring Routing Policies 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Configuration Task Summary 3
1.3 Configuring a Filter List 4
1.3.1 Overview 4
1.3.2 Restrictions and Guidelines 4
1.3.3 Configuration Tasks 4
1.3.4 Defining AS Path Filtering Rules 4
1.3.5 Defining a Community List 5
1.3.6 Defining an Extcommunity List 5
1.3.7 Creating a Prefix List 6
1.3.8 Adding a Text Description for a Prefix List 6
1.3.9 Displaying Sequence Numbers in a Prefix List 7
1.3.10 Creating an IPv6 Prefix List 7
1.3.11 Adding a Text Description for an IPv6 Prefix List 8
1.3.12 Displaying Sequence Numbers in an IPv6 Prefix List 8
1.4 Configuring a Route Map 8
1.4.1 Overview 8
1.4.2 Configuration Tasks 9

1.4.3 Creating a Policy 9

1.4.4 Configuring the Matching Conditions of a Rule 9

1.4.5 Configuring the Processing Actions of a Policy 12

1.5 Monitoring 16

1.6 Configuration Examples 17

1.6.1 Applying Rules Configured in a Route Map During Route Redistribution 17

1.6.2 Applying a Route Map in PBR 20

1.6.3 Configuring a Prefix List 23

1.6.4 Configuring an AS-Path List 25

1.6.5 Configuring a Community List 27

1 Configuring Routing Policies

1.1 Introduction

1.1.1 Overview

Routing policies are a policy set for changing the packet forwarding path or routing information and are often implemented by a filter list and a route map. Routing policies provide services for different routing protocols, and completes the policy-based control of routing information based on a specified policy set. Policy-based routing (PBR) refers to policy-based routing and forwarding. It can forward packets based on the source address, destination address, packet length, and port, and these matching policies can be provided by routing policies.

Routing policies are flexibly and widely applied in the following ways:

- A filter list is used in a routing protocol to filter or modify routing information.
- A route map is used in a routing protocol to filter or modify routing information. The route map can further use a filter list.
- A route map is used in PBR to control packet forwarding or modify packet fields.

Note

In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be Layer-3 switches, routers, or firewalls.

1.1.2 Principles

Filter list: It is a group of lists defined based on a routing attribute and can be used by a routing protocol for route filtering.

Route map: It defines a policy that "if certain conditions are matched, processing actions are performed accordingly."

1. Filter List

A filter list is a group of lists defined based on a routing attribute and is a filtering tool of routing policies. To achieve the effect of route filtering, filter lists must be used in a routing protocol or route map. Five types of filter lists are available currently: access control list (ACL), prefix list, autonomous system (AS) path list, community list, and extended community (extcommunity) list.

- ACL

  ACLs include IPv4 and IPv6 ACLs. When defining an ACL, you can specify IPv4/IPv6 addresses and masks to match the destination network segment or next-hop addresses of routing information.

- Prefix list

Similar to ACLs, prefix lists, including IPv4 prefix lists and IPv6 prefix lists, are used to match destination network segments or next hops of routing information.

When configuring a prefix list as the filter list, you can define the prefix address, mask length, and mask range. The prefix address and mask length are used to specify the prefix of the routing information. The mask range specifies the mask range of the routing information to be filtered. That is, a prefix list can be defined to directly filter the subnet segment under a specified prefix network segment without calculating the prefix of the subnet segment in advance. Therefore, prefix lists are more flexible than ACLs.

- AS-path list

  AS-path lists are applicable only to Border Gateway Protocol (BGP). They define filtering rules based on the AS path information. When configuring an AS-path list, you can specify an AS path by using a regular expression to match the AS path.

- Community list

Community lists are applicable only to BGP. They define filtering rules based on the community attributes of routes. When configuring a community list, you can specify a community ID or a regular expression to match the community attribute.

- Extcommunity list

Extcommunity lists are applicable only to BGP. They define filtering rules based on the extended community attributes of routes. When configuring an extcommunity list, you can specify an extended community ID or a regular expression to match the extended community attribute.

2. Route Map

A policy in a route map is a match and set statement, which indicates that if certain conditions are matched, some processing actions will be performed accordingly.

- Main application scenarios of route maps
  - Route filtering: A filter list is used in a routing protocol to filter the routing information sent or received by the protocol.
  - Route redistribution: A route map is used in a routing protocol to filter or modify routing information and redistribute Routing Information Protocol (RIP) routes to Open Shortest Path First (OSPF). Only RIP routes with the hop count of 4 can be redistributed.
  - PBR: A route map is used in PBR to control packet forwarding or modify packet fields and specify optimum outbound interfaces for packets from different subnets.
- Policy execution

  A route map contains multiple policies. Each policy has a corresponding sequence number. A smaller sequence number means a higher priority. You can execute policies by sequence number. Once the matching condition of a policy is met, the processing action of this policy is performed and the route map exits. If no matching condition of any policy is met, no processing action is performed.

- Working modes of policies

  Policies support two working modes:

- **permit**: When the matching condition of a policy is met, the processing action for this policy is performed and the system exits the route map.
- **deny**: When the matching condition of a policy is met, the processing action for this policy is not performed and the system exits the route map.

- Matching conditions of policies

  The matching condition of a policy may contain zero, one, or more match rules.

  - If the matching condition contain zero match rules, all packets match the policy.
  - If the matching condition contains one or more match rules, the matching condition is met only when all the rules are matched.

- Processing action for a policy

  The processing action of a policy may contain zero, one, or more set rules.

  - If the processing action contains zero set rules, no processing action is performed and the system directly exits the route map.
  - If the processing action contains one or more set rules, all processing actions are performed and then the system exits the route map.

1.2 Configuration Task Summary

The configuration of a routing policy includes the following tasks:

(1) (Optional) Configuring a Filter List

- Defining AS Path Filtering Rules
- Defining a Community List
- Defining an Extcommunity List
- Creating a Prefix List
- Adding a Text Description for a Prefix List
- Displaying Sequence Numbers in a Prefix List
- Creating an IPv6 Prefix List
- Adding a Text Description for an IPv6 Prefix List
- Displaying Sequence Numbers in an IPv6 Prefix List

(2) Configuring a Route Map

a Creating a Policy

b Configuring the Matching Conditions of a Rule

c Configuring the Processing Actions of a Policy

1.3 Configuring a Filter List

1.3.1 Overview

This section describes how to define a set of route filtering rules for a routing protocol.

1.3.2 Restrictions and Guidelines

A configured filter list can take effect only after it is associated with a routing protocol.

1.3.3 Configuration Tasks

The filter list configuration includes the following tasks. All the configuration tasks below are optional. Select the configuration tasks as required.

- Defining AS Path Filtering Rules
- Defining a Community List
- Defining an Extcommunity List
- Creating a Prefix List
- Adding a Text Description for a Prefix List
- Displaying Sequence Numbers in a Prefix List
- Creating an IPv6 Prefix List
- Adding a Text Description for an IPv6 Prefix List
- Displaying Sequence Numbers in an IPv6 Prefix List

1.3.4 Defining AS Path Filtering Rules

1. Overview

An AS path filter list defines AS path filtering rules by using regular expressions. AS-path is a BGP attribute. Therefore, defined AS path filtering rules are applied to a BGP network.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Define AS path filtering rules.

ip as-path access-list *path-list-num* { **permit** | **deny** } *regular-expression*

By default, no AS path filtering rule is configured.

1.3.5 Defining a Community List

1. Overview

A community is a set of routes with the same characteristics. Community attributes are BGP attributes and can help reduce the difficulties in BGP route management and maintenance. Similar to an ACL, you can define multiple entries in a community list, and entries are matched based on their sequence numbers. As long as routes match one entry, the routes are permitted by the community list and no further matching is performed.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Define a standard community list.

ip community-list { *community-list-number* | **standard** *community-list-name* } { **permit** | **deny** } [{ *community-list-number* | **internet** | **local-AS** | **no-advertise** | **no-export** | **gshut** }]

By default, no standard community list is defined.

(4) Define an expanded community list.

ip community-list { *community-list-number* | **expanded** *community-list-name* } { **permit** | **deny** } [*regular-expression*]

By default, no expanded community list is defined.

1.3.6 Defining an Extcommunity List

1. Overview

An extended community is a set of routes with the same characteristics. Extended community attributes are BGP attributes and can help reduce the difficulties in BGP route management and maintenance. Similar to an ACL, you can define multiple entries in an extcommunity list, and entries are matched based on their sequence numbers. As long as routes match one entry, the routes are permitted by the extcommunity list and no further matching is performed.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Define a standard extcommunity list.

ip extcommunity-list { *standard-list* | **standard** *list-name* } { **permit** | **deny** } [**rt** *rt-value* | **soo** *soo-value*]

By default, no standard extcommunity list is defined.

(4) Define an expanded extcommunity list.

ip extcommunity-list { *expanded-list* | **expanded** *list-name* } { **permit** | **deny** } [*regular-expression*]

By default, no expanded extcommunity list is defined.

1.3.7 Creating a Prefix List

1. Overview

Prefix lists can be directly used by protocols, or used together with a route map as a matching condition of the route map. Similar to an ACL, you can define multiple entries in a prefix list, and entries are matched based on their sequence numbers. As long as routes match one entry, the routes are permitted by the prefix list and no further matching is performed. If routes do not match any entry, it is considered that the routes are denied by the prefix list.

2. Restrictions and Guidelines

This command is not a routing policy command, and will not be applied to any routing protocol.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a prefix list.

ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv4-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

By default, no prefix list is configured.

1.3.8 Adding a Text Description for a Prefix List

1. Overview

You can add a text description for a prefix list, for example, to describe the purpose of the prefix list. Adding text descriptions for prefix lists can facilitate maintenance and tracking.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Add a text description for a prefix list.

ip prefix-list *prefix-list-name* **description** *description-text*

By default, no text description is configured for a prefix list.

1.3.9 Displaying Sequence Numbers in a Prefix List

1. Overview

When you run the **show ip prefix-list** command, the sequence numbers of entries in a prefix list are not displayed by default. If these sequence numbers are displayed, you can conveniently add or remove an entry to or from the prefix list.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of displaying sequence numbers in a prefix list.

ip prefix-list sequence-number

By default, the function of displaying sequence numbers in a prefix list is disabled.

1.3.10 Creating an IPv6 Prefix List

1. Overview

Prefix lists can be directly used by protocols, or used together with a route map as a matching condition of the route map. Similar to an ACL, you can define multiple entries in a prefix list and entries are matched based on their sequence numbers. As long as routes match one entry, the routes are permitted by the prefix list and no further matching is performed. If routes do not match any entry, it is considered that the routes are denied by the prefix list.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an IPv6 prefix list.

ipv6 prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

By default, no IPv6 prefix list is configured.

1.3.11 Adding a Text Description for an IPv6 Prefix List

1. Overview

You can add a text description for a prefix list, for example, to describe the purpose of the prefix list. Adding text descriptions for prefix lists can facilitate maintenance and tracking.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Add a text description for an IPv6 prefix list.

ipv6 prefix-list *prefix-list-name* **description** *description-text*

By default, no text description is configured for an IPv6 prefix list.

1.3.12 Displaying Sequence Numbers in an IPv6 Prefix List

1. Overview

When you run the **show ipv6 prefix-list** command, the sequence numbers of entries in a prefix list are not displayed by default. If these sequence numbers are displayed, you can conveniently add or remove an entry to or from the prefix list.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of displaying sequence numbers in an IPv6 prefix list.

ipv6 prefix-list sequence-number

By default, the function of displaying sequence numbers in an IPv6 prefix list is displayed.

1.4 Configuring a Route Map

1.4.1 Overview

This section describes how to define a set of routing policies to be used by routing protocols or PBR.

1.4.2 Configuration Tasks

The route map configuration includes the following tasks:

(1) Creating a Policy

(2) Configuring the Matching Conditions of a Rule

(3) Configuring the Processing Actions of a Policy

1.4.3 Creating a Policy

1. Overview

You can create a route map to control route attributes.

2. Restrictions and Guidelines

- If the route map is unavailable, this command will create a route map and add a policy to the route map.
- If the route map is available, this command will add a policy to the route map.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a route map and enter the route map configuration mode.

route-map *route-map-name* [{ **permit** | **deny** } *sequence*]

1.4.4 Configuring the Matching Conditions of a Rule

1. Overview

In a route map, you can configure match rules based on the route attributes. If multiple match rules are configured, all the rules must be matched.

2. Restrictions and Guidelines

- If you use an ACL in a **match** command to define packet matching conditions, you must configure this ACL.
- The following table lists the **match** commands that cannot be configured at the same time:

Table 1-1 Match Commands That Cannot Be Configured at the Same Time

match Command	Exclusive match Command
match ip address	**match ip prefix-list**

match Command	Exclusive match Command
match ipv6 address	**match ipv6 prefix-list**
match ip next-hop	**match ip next-hop prefix-list**
match ipv6 next-hop	**match ipv6 next-hop prefix-list**
match ip route-source	**match ip route-source prefix-list**
match ipv6 route-source	**match ipv6 route-source prefix-list**

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the route map configuration mode.

route-map *route-map-name* [{ **permit** | **deny** } *sequence*]

(4) Configure a rule to match the next-hop outbound interface.

match interface { *interface-type interface-number* }&<1-4>

By default, traffic is not matched with an interface that is used as the next-hop outbound interface.

Use an IPv4 filter list in the route map to match attributes. The following configurations are optional. You can configure multiple match rules, all of which must be matched.

- Configure an AS-path list for packet matching.

  match as-path *as-path-acl-list-number*&<1-10>

  By default, no AS-path list is configured for packet matching.

- Configure a community list as a match rule.

  match community { *community-list-number* | *community-list-name* } [**exact-match** | *community-list-number* | *community-list-name*]&<1-6>

  By default, no community list is configured for packet matching.

- Configure an extcommunity list for packet matching.

  match extcommunity { *standard-list-number* | *standard-list-name* | *expanded-list-num* | *expanded-list-name* }&<1-6>

  By default, no extcommunity list is configured for packet matching.

- Configure a rule to match the target network routes that are permitted in the ACL or prefix list.

  match ip address { { *acl-number* | *acl-name* } &<1-6> | **prefix-list** *prefix-list-name*&<1-6> }

By default, no ACL or prefix list used for packet matching is configured.

- Configure a rule to match the target network routes whose next-hop IPv4 addresses meet rules in the ACL or prefix list.

  match ip next-hop { { *acl-number* | *acl-name* } &<1-6> | **prefix-list** *prefix-list-name*&<1-6> }

  By default, no ACL or prefix list used for next-hop IP address matching is configured.

- Configure a rule to match the target network routes of a specified L3 authentication traffic diversion domain type.

  match ip policy { *acl-number* | *acl-name* }&<1-6> **class** *class-id*

- Configure a rule to match the target network routes whose source IP addresses meet rules in the ACL or prefix list.

  match ip route-source { { *acl-number* | *acl-name* } &<1-6> | **prefix-list** *prefix-list-name*&<1-6> }

  By default, no ACL or prefix list is configured to match the source IP addresses of routes.

(5) Use an IPv6 filter list in the route map to match attributes.

- Configure a rule to match the target IPv6 network routes that are permitted in the ACL or prefix list.

  match ipv6 address { *acl-name* | **prefix-list** *prefix-list-name* }

  By default, no IPv6 ACL or IPv6 prefix list is configured for packet matching.

- Configure a rule to match the target network routes whose next-hop IPv6 addresses meet rules in the ACL or prefix list.

  match ipv6 address { *acl-name* | **prefix-list** *prefix-list-name* }

  By default, no IPv6 ACL or IPv6 prefix list is configured for next-hop IP address matching.

- Configure a rule to match the target network routes whose source IPv6 addresses meet rules in the ACL or prefix list.

  match ipv6 route-source { *acl-name* | **prefix-list** *prefix-list-name* }

  By default, no IPv6 ACL or IPv6 prefix list is configured to match the source IP addresses of routes.

(6) Configure a rule to match the routes with a fixed metric.

match metric *metric*

By default, the metric values of routes are not matched.

(7) Configure a rule to match the route type.

- Configure a rule to match the BGP route source.

  match origin { **egp** | **igp** | **incomplete** }

  By default, no rule is configured to match any source routes.

- Configure a rule to match the route type.

  match route-type { **static** | **connect** | **rip** | **local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2** | **evpn-type-1** | **evpn-type-2** | **evpn-type-3** | **evpn-type-4** | **evpn-type-5** }

  By default, no rule is configured to match any route type.

(8) Configure a rule to match the routes with a specified tag.

match tag *tag*&<1-4>

1.4.5 Configuring the Processing Actions of a Policy

1. Overview

Processing actions are configured for traffic that matches the rules. The device provides abundant **set** commands for setting flexible processing actions.

2. Restrictions and Guidelines

- If no set rule is configured, no processing action will be performed.
- If multiple set rules are configured, all set rules must be executed. If the set rules have different priorities, only the set rule with the highest priority takes effect.
- The following table lists the **set** commands that cannot be configured at the same time.

Table 1-2 set Commands That Cannot Be Configured at the Same Time

set Command	Exclusive set Command
set ip next-hop	**set ip next-hop verify-availability**
set ip dscp	**set ip tos**
set ip dscp	**set ip precedence**

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the route map configuration mode.

route-map *route-map-name* [{ **permit** | **deny** } *sequence*]

(4) Configure a rule to adjust the BGP attributes.

- Configure the AS number for BGP.

  set aggregator as *as-number ipv4-address*

  By default, no AS number of the aggregator is specified.

- Configure the Accumulated Interior Gateway Protocol (AIGP) metric attribute for Exterior Gateway Protocol (EGP).

set aigp-metric { *metric-number* | **igp-metric** }

By default, no AIGP metric attribute is configured for routes.

- Configure a rule to add the specified AS_PATH values.

  set as-path prepend *as-number*&<1-10>

  By default, no rule is configured to add AS_PATH values for routes.

- Configure a rule to replace the AS_PATH attributes of routes.

  set as-path replace *as-number*&<1-10>

  By default, the AS_PATH values of matched routes will not be replaced.

- Configure the atomic-aggregate attribute for routes.

  set atomic-aggregate

  By default, no atomic-aggregate attribute is configured for routes.

- Configure a rule to delete all the community values from BGP routes matching the rules according to the community list.

  set comm-list { *community-list-number* | *community-list-name* } **delete**

  By default, no rule is configured to delete all the community values from routes matching the rules according to the community list.

- Configure the community value for BGP routes.

  set community { **none** | { *community-number* | **internet** | **local-AS** | **no-advertise** | **no-export** }&<1-32> [**additive**] }

  By default, no community value is specified for a route.

- Configure the flapping parameters for BGP routes.

  set dampening *half-life reuse suppress max-suppress-time*

  By default, when the half-life period is 15 minutes, and the penalty value of a route is lower than 750, route suppression is canceled. When the penalty value of a route exceeds 2000, the route is suppressed. A route can be suppressed for a maximum of 60 minutes.

- Configure a rule to delete the extended community attribute of BGP routes.

  set extcomm-list { *extcommunity-list-number* | *extcommunity-list-name* } **delete**

- Configure the extended community attribute of BGP routes.

  set extcommunity { **rt** *extend-community-value* | **soo** *extend-community-value* }

(5) Configure the backup outbound interface and backup next hop for fast reroute (FRR).

- Configure the backup outbound interface and backup next hop for FRR.

  set fast-reroute backup-interface *interface-type interface-number* **backup-nexthop** *ipv4-address*

  By default, no backup outbound interface and backup next hop of FRR are specified for matched routes.

(6) Configure the next hop.

- Configure the default next-hop IPv4 address for routes.

set ip default next-hop { *ipv4-address* [*weight*] }&<1-32>

By default, no default next-hop IPv4 address is specified for matched routes.

- Configure the next-hop IPv4 address for IPv4 packets.

  set ip next-hop { *ipv4-address* [*weight*] }&<1-32>

  By default, no next-hop IPv4 address is specified for matched packets.

- Configure the next-hop IP address for routes.

  set next-hop *ipv4-address*

  By default, no next-hop IP address is specified for matched routes.

- Configure the default next-hop IPv6 address for an IPv6 packet.

  set ipv6 default next-hop { *ipv6-address* [*weight*] }&<1-32>

  By default, no default next-hop IPv6 address is specified for matched IPv6 routes.

- Configure the next-hop IPv6 address for an IPv6 packet.

  set ipv6 next-hop { *ipv6-address* [*weight*] }&<1-32>

- Configure the recursive next-hop IP address for packets.

  set ip next-hop recursive *ipv4-address*

  By default, no recursive next-hop IPv4 address is specified for matched packets.

- Set the next hops of routes to the device itself.

  set ip next-hop self

  By default, the next hop is not set to the device itself for matched packets.

- Set the next hop of a route to keep unchanged.

  set ip next-hop unchanged

  By default, the next hop is not set to keep unchanged for matched packets.

- Set the next hop of a route to the device itself.

  set next-hop self

  By default, the next hop is not set to the device itself for matched routes.

- Set the next hop of the specified route to keep unchanged.

  set next-hop unchanged

  By default, the next hop is not set to keep unchanged for matched routes.

- Configure the recursive next-hop IPv6 address.

  set ipv6 next-hop recursive *ipv6-address*

  By default, no recursive next-hop IPv6 address is specified for matched IPv6 packets.

- Set the next hop of the specified IPv6 route to the device itself.

  set ipv6 next-hop self

  By default, the next hop address is not set to the device itself for matched IPv6 packets.

- Set the next hop of the specified IPv6 route to keep unchanged.

  set ipv6 next-hop unchanged

  By default, the next hop is not set to keep unchanged for matched IPv6 packets.

- Set the L3 VPN next hop to the local virtual routing and forwarding (VRF) instance.

  set l3vpn nexthop local-vrf

By default, the L3 VPN next hop is not set to the local VRF instance for routes matching the rules.

- Verify availability of the next-hop IPv4 address.

  set ip next-hop verify-availability *ipv4-address* [*weight*] { **track** *track-obj-number* | **bfd** *interface-type interface-number gateway* }

  By default, availability of the next-hop IPv4 address is not verified for matched packets.

- Verify availability of the next-hop IPv6 address.

  set ipv6 next-hop verify-availability *ipv6-address* [*weight*] **bfd** *interface-type interface-number gateway*

  By default, availability of the next-hop IPv6 address is not verified for matched packets.

(7) Configure the flow control parameters.

- Configure the IPv4 header priority.

  set ip precedence { *precedence* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine** }

  By default, no IPv4 header priority is configured for matched packets.

- Configure the IPv6 header priority.

  set ipv6 precedence { *precedence-number* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine** }

  By default, no IPv6 header priority is configured for matched packets.

- Configure the type of service (ToS) for the IPv4 header of a packet.

  set ip tos { *tos-number* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal** }

  By default, no ToS is configured for the IP header of a matched packet.

- Configure the LOCAL_PREFERENCE parameter.

  set local-preference *precedence-number*

  By default, no LOCAL_PREFERENCE value is configured for matched routes.

- Configure the quality of service (QoS) ID for a route.

  set qos-id *qos-id*

  By default, no QoS ID is specified for matched routes.

- Configure the Differentiated Services Code Point (DSCP) in an IPv4 packet.

  set ip dscp *dscp_value*

  By default, no DSCP is configured in an IPv4 packet for matched routes.

(8) Configure redistribution-related information.

- Configure the type of the destination area to which redistributed routes are to be advertised.

  set level { **level-1** | **level-1-2** | **level-2** | **stub-area** | **backbone** }

  By default, the type of the destination area is not specified for matched routes.

- Configure the redistributed route tag.

  set tag *tag*

  By default, no route tag is configured for matched routes.

(9) Configure the weight, metric, and metric type.

- Configure the metric for routes.

  set metric { **+** *metric-value* | **-** *metric-value* | *metric-value* }

  By default, the metric of a matched route is not modified.

- Configure the metric type for routes.

  set metric-type { **external** | **internal** | **type-1** | **type-2** }

- Configure the weight for BGP routes.

  set weight *weight-number*

  By default, no weight is configured for matched routes.

(10) Configure the route source information.

- Configure the route source attribute.

  set origin { **egp** | **igp** | **incomplete** }

  By default, no route source is specified for matched routes.

- Configure the route originator address.

  set originator-id *ipv4-address*

  By default, no route originator address is configured for matched routes.

(11) Configure the route management distance.

set distance *distance-number*

By default, no management distance is modified for matched routes.

1.5 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-3 Routing Policy Monitoring

Command	Purpose
show route-map [*route-map-name*]	Displays the configurations of a route map.

Command	Purpose
show access-lists [*acl-id* | *name*]	Displays the configurations of an ACL.
show ip prefix-list [*prefix-name*]	Displays the configurations of an IPv4 prefix list.
show ip protocols [**vrf** *vrf-name*] [**bgp** | **isis** | **ospf** | **rip**]	Displays the status of the IPv4 routing protocols that are currently running.
show ipv6 prefix-list [*prefix-name*]	Displays the configurations of an IPv6 prefix list.
show ip as-path-access-list [*as-path-access-list-num*]	Displays the configurations of an AS-path list.
show ip community-list [*community-list-number* | *community-list-name*]	Displays the configurations of a community list.
show ip extcommunity-list [*extcommunity-list-num* | *extcommunity-list-name*]	Displays the configurations of an extcommunity list.

1.6 Configuration Examples

1.6.1 Applying Rules Configured in a Route Map During Route Redistribution

1. Requirements

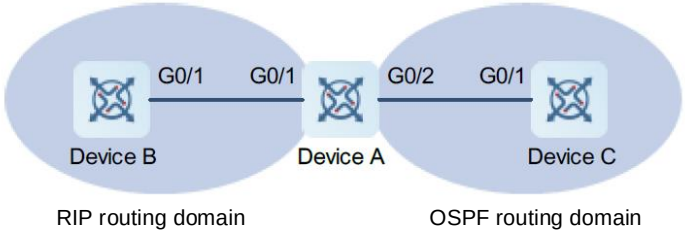
The RIP routing domain needs to exchange routes with the OSPF routing domain to realize the network-wide interworking.

When RIP routes are redistributed to OSPF, the routes with too many hops are considered unreliable. Therefore, it is required that only RIP routes with the hop count of 4 be redistributed. In the OSPF routing domain, if a route is a Type-1 external route, the tag value of the route is set to 40.

When OSPF routes are redistributed to RIP, only OSPF routes with the tag value of 10 are redistributed. In the RIP routing domain, the initial metric of the routes redistributed to RIP is set to 10.

2. Topology

Figure 1-1 Topology of Route Map Application During Route Redistribution



3. Notes

- Configure the route map **redrip** as follows: Configure a rule to match routes with the hop count of 4, set the initial metric of the routes to **40**, set the route type to the external route **type-1**, and set the tag of the routes to **40**.
- Configure the route map **redospf** as follows: Configure a rule to match routes with the tag of **10** and set the initial metric of the routes to **10**.
- Apply the route map **redrip** when RIP routes are redistributed to OSPF.
- Apply the route map **redospf** when OSPF routes are redistributed to RIP.

4. Procedure

(1) Configure IP addresses of the interfaces, and complete the basic OSPF and RIP configuration. (Omitted)

(2) Configure a route redistribution policy for OSPF. In the policy, configure a rule to match routes with the hop count of 4, set the route type to **Type-1** and the tag to **40**.

```
Device A> enable
Device A# configure terminal
Device A(config)# route-map redrip permit 10
Device A(config-route-map)# match metric 4
Device A(config-route-map)# set metric-type type-1
Device A(config-route-map)# set tag 40
Device A(config-route-map)# exit
```

(3) Configure a route redistribution policy for RIP. In the policy, configure a rule to match routes with the route tag of **10** and set the metric to **10**.

```
Device A(config)# route-map redospf permit 10
Device A(config-route-map)# match tag 10
Device A(config-route-map)# set metric 10
Device A(config-route-map)# exit
```

(4) Configure redistribution of RIP routes to OSPF, and use the route map **redrip** for routing control.

```
Device A(config)# router ospf 1
```

```
Device A(config-router)# redistribute rip subnets route-map redrip
Device A(config-router)# exit
```

(5) Configure the redistribution of OSPF routes to RIP, and use the route map **redospf** for routing control.

```
Device A(config)# router rip
Device A(config-router)# redistribute ospf 1 route-map redospf
Device A(config-router)# exit
```

5. Verification

Check the route map configurations on device A to verify the policy rules.

```
Device A# show route-map
route-map redrip, permit, sequence 10
  Match clauses:
    metric 4
  Set clauses:
    metric 40
    metric-type type-1
    tag 40
route-map redospf, permit, sequence 10
  Match clauses:
    tag 10
  Set clauses:
metric 10
```

Check the OSPF routing information library on device A to verify that the routes matching the policy rules are redistributed.

```
Device A# show ip ospf database external

          OSPF Router with ID (192.100.1.9) (Process ID 1)

              AS External Link States

  LS age: 5
  Options: 0x2 (-|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 192.168.199.0 (External Network Number)
  Advertising Router: 192.100.1.9
  LS Seq Number: 80000001
  Checksum: 0x554d
  Length: 36
  Network Mask: /24
       Metric Type: 1
       TOS: 0
```

```
      Metric: 4
      Forward Address: 0.0.0.0
      External Route Tag: 40
```

6. Configuration Files

Device A configuration file

```
!
route-map redrip permit 10
 match metric 4
 set metric-type type-1
 set tag 40
!
route-map redospf permit 10
 match tag 10
 set metric 10
!
router ospf 1
redistribute rip route-map redrip subnets
!
router rip
redistribute ospf 1 route-map redospf
!
```

1.6.2 Applying a Route Map in PBR

1. Requirements

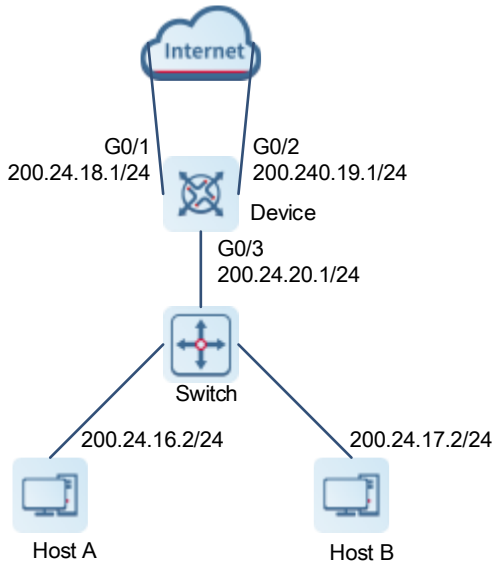
Configure PBR on the devices to achieve the following purposes:

- Packets from subnet 1 (200.24.16.0/24) are sent from GE0/1 first.
- Packets from subnet 2 (200.24.17.0/24) are sent from GE0/2 first.

The two egress links work in mutual backup mode.

2. Topology

Figure 1-2 Topology of Route Map Application in PBR



3. Notes

- Configure two different ACLs to match packets from subnets 1 and 2 respectively.
- Configure the route map RM_FOR_PBR: Configure policy 10 to ensure that "packets from host A are sent from GigabitEthernet 0/1 first"; configure policy 20 to ensure that "packets from host B are sent from GigabitEthernet 0/2 first".
- Configure PBR and apply the route map RM_FOR_PBR to packets received from GigabitEthernet 0/3.
- Configure a PBR to implement redundant backup among multiple next hops.

4. Procedure

(1) Configure the IP addresses of interfaces to implement interworking between networks. (Omitted)

(2) Configure ACLs for subnets 200.24.16.0/24 and 200.24.17.0/24, respectively.

```
Device> enable
Device# configure terminal
Device(config)# access-list 1 permit 200.24.16.0 0.0.0.255
Device(config)# access-list 2 permit 200.24.17.0 0.0.0.255
```

(3) Configure the routing map **RM_FOR_PBR**, set the next hop of 200.24.16.0 to 200.24.18.1 and its backup next hop to 200.24.19.1, and set the next hop of 200.24.17.0 to 200.24.19.1 and its backup next hop to 200.24.18.1.

```
Device(config)# route-map RM_FOR_PBR 10
Device(config-route-map)# match ip address 1
Device(config-route-map)# set ip next-hop 200.24.18.1
```

```
Device(config-route-map)# set ip next-hop 200.24.19.1
Device(config-route-map)# exit
Device(config)# route-map RM_FOR_PBR 20
Device(config-route-map)# match ip address 2
Device(config-route-map)# set ip next-hop 200.24.19.1
Device(config-route-map)# set ip next-hop 200.24.18.1
Device(config-route-map)# exit
```

(4) Apply the route map **RM_FOR_PBR** to the interface GigabitEthernet 0/3, and enable load balancing.

```
Device(config)# interface GigabitEthernet 0/3
Device(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR
Device(config-if-GigabitEthernet 0/3)# exit
Device(config)# ip policy redundance
```

5. Verification

Check the PBR configurations to verify that the route map is applied to the interface.

```
Device# show ip policy
Balance mode: redundance
Interface                          Route map
GigabitEthernet 0/3                  RM_FOR_PBR
```

Check the configurations of the route map to verify the policy rules.

```
Device# show route-map
route-map RM_FOR_PBR, permit, sequence 10
  Match clauses:
    ip address 1
  Set clauses:
    ip next-hop 200.24.18.1
    ip next-hop 200.24.19.1
route-map RM_FOR_PBR, permit, sequence 20
  Match clauses:
    ip address 2
  Set clauses:
    ip next-hop 200.24.19.1
    ip next-hop 200.24.18.1
```

Check the ACL configurations to verify the packet filtering rules.

```
Device# show access-lists
ip access-list standard 1
 10 permit 200.24.16.0 0.0.0.255
 10 permit 200.24.16.0 0.0.0.255
ip access-list standard 2
 10 permit 200.24.17.0 0.0.0.255
```

6. Configuration Files

Device configuration file

```
!
ip policy redundance
!
access-list 1 permit 200.24.16.0 0.0.0.255
access-list 2 permit 200.24.17.0 0.0.0.255
!
route-map RM_FOR_PBR 10
 match ip address 1
 set ip next-hop 200.24.18.1
 set ip next-hop 200.24.19.1
!
route-map RM_FOR_PBR 20
 match ip address 2
 set ip next-hop 200.24.19.1
 set ip next-hop 200.24.18.1
!
interface GigabitEthernet 0/3
 ip policy route-map RM_FOR_PBR
!
```

7. Common Errors

- After a policy that uses ACLs and prefix-lists for matching is configured, the corresponding ACLs and prefix lists are not defined.

1.6.3 Configuring a Prefix List

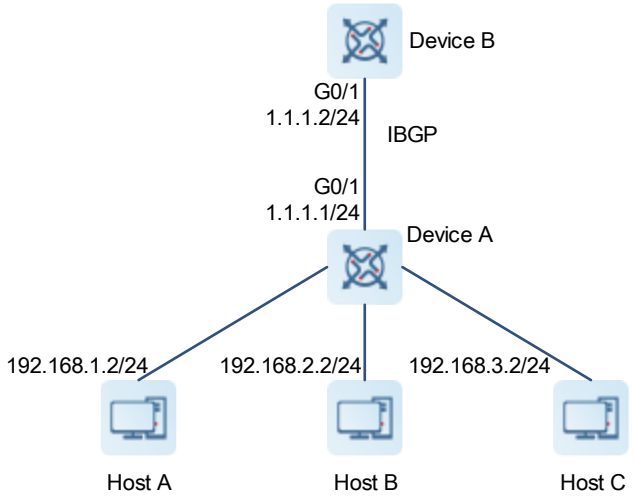
1. Requirements

Device A and device B are Interior Border Gateway Protocol (IBGP) neighbors.

On device A, perform routing control so that only routes in the 192.168.1.0/24 network segment are advertised to device B.

2. Topology

Figure 1-3 Topology of the Prefix List Function



3. Notes

- Configure device A and device B as IBGP neighbors and configure device A to advertise routes to the connected three subnets.
- Configure a prefix list.
- Associate the prefix list with device A to filter sent routes.

4. Procedure

(1) Configure the IP addresses of interfaces, and configure device A and device B to advertise routes and become IBGP neighbors. (Omitted)

(2) Configure a prefix list to match the traffic of 192.168.1.0/24.

```
Device A> enable
Device A# configure terminal
Device A(config)# ip prefix-list pre1 permit 192.168.1.0/24
```

(3) Specify the neighbor 1.1.1.2 in BGP, and apply the prefix list **pre1** to filter sent routes.

```
Device A(config)# router bgp 100
Device A(config-router)# neighbor 1.1.1.2 prefix-list pre1 out
```

5. Verification

Check the prefix list.

```
Device A> enable
Device A# show ip prefix-list
```

```
ip prefix-list pre1: 1 entries
    seq 5 permit 192.168.1.0/24

Device A# show ip bgp
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, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric     LocPrf     Weight Path
*> 192.168.1.0      0.0.0.0                0                32768    i
*> 192.168.2.0      0.0.0.0                0                32768    i
*> 192.168.3.0      0.0.0.0                0                32768    i

Total number of prefixes 3
```

Check the BGP routing table to verify that the routes are filtered correctly.

```
Device B> enable
Device B# show ip bgp
BGP table version is 4, local router ID is 1.1.1.2
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
*>i192.168.1.0      1.1.1.1            0        100          0    i

Total number of prefixes 1
```

6. Configuration Files

- Device A configuration file

```
!
ip prefix-list pre1 permit 192.168.1.0/24
!
router bgp 100
neighbor 1.1.1.2 prefix-list pre1 out
!
```

1.6.4 Configuring an AS-Path List

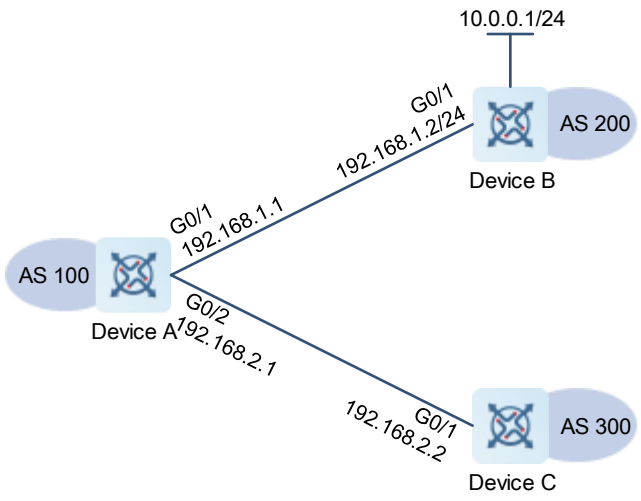
1. Requirements

Device A, device B, and device C are Exterior Border Gateway Protocol (EBGP) neighbors.

Device A filters the routes that are received from device B and device C and contain the AS number of 200.

2. Topology

Figure 1-4 Topology of the AS-Path List Function



3. Notes

- Create an AS-path filtering rule to match path information containing only the AS number of 200.
- On device A, establish the EBGP neighborship with device B and device C.
- Associate an AS-path list with device A to filter the routes received from device B and device C.

4. Procedure

(1) Configure IP addresses of the interfaces, and complete the basic EBGP configuration. (Omitted)

(2) Configure an AS-path list to match routes with the AS number of 200.

```
Device A(config)# ip as-path access-list 123 permit ^200$
```

(3) On device A, specify the BGP neighbors, and use the AS path list **123** to filter routes.

```
Device A(config)# router bgp 100
Device A(config-router)# neighbor 192.168.1.2 filter-list 123 in
Device A(config-router)# neighbor 192.168.2.2 filter-list 123 in
```

5. Verification

Check the AS-path list.

```
Device A> enable
Device A# show ip as-path-access-list
AS path access list 123
permit ^200$
```

Before associating the AS-path list, check the BGP routing table to verify that all routes are learned.

```
Device A# show ip bgp
BGP table version is 1, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric     LocPrf     Weight Path
*> 10.0.0.0/24      192.168.1.2             0                    0 200 i
*> 20.0.0.0/24      192.168.2.2             0                    0 300 i

Total number of prefixes 2
```

After associating the AS path list with device A, check the BGP routing table to verify that routes are filtered correctly.

```
Device A# show ip bgp
BGP table version is 1, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric     LocPrf     Weight Path
*> 10.0.0.0/24      192.168.1.2             0                    0 200 i
Total number of prefixes 1
```

6. Configuration Files

- Device A configuration file

```
!
ip as-path access-list 123 permit ^200$
!
router bgp 100
neighbor 192.168.1.2 filter-list 123 in
neighbor 192.168.2.2 filter-list 123 in
!
```

1.6.5 Configuring a Community List

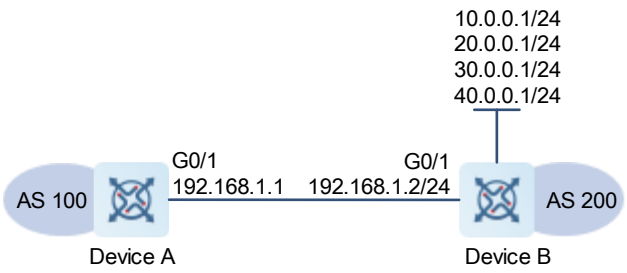
1. Requirements

Device A and device B are EBGP neighbors.

Device A filters routes received from device B, and receives only routes with the community attribute of **100:20**.

2. Topology

Figure 1-5 Topology of the Community List Function



3. Notes

- Define a standard community list to match routes with the community attribute of **100:20**.
- Establish the EBGP neighborship between device A and device B.
- Configure device B to advertise routes with the community attribute.
- Associate the community list on device A (BGP can be applied only through a route map) to filter routes received from device B.

4. Procedure

(1) Configure IP addresses of the interfaces, and complete the related basic configuration. (Omitted)

(2) Configure a route map on device B, and set the community attribute.

```
Device B> enable
Device B# configure terminal
Device B(config)# route-map comm1
Device B(config-route-map)# set community 100:20 200:20
Device B(config-route-map)# exit
Device B(config)# route-map comm2
Device B(config-route-map)# set community 100:20
Device B(config-route-map)# exit
Device B(config)# route-map comm3
Device B(config-route-map)# set community 200:20
Device B(config-route-map)# exit
```

(3) Configure device B to advertise routes with the community attribute.

```
Device B(config)# router bgp 200
Device B(config-router)# neighbor 192.168.1.1 send-community
Device B(config-router)# network 10.0.0.0 mask 255.255.255.0 route-map comm1
Device B(config-router)# network 20.0.0.0 mask 255.255.255.0 route-map comm2
Device B(config-router)# network 30.0.0.0 mask 255.255.255.0 route-map comm3
```

```
Device B(config-router)# network 40.0.0.0 mask 255.255.255.0
```

(4) On device A, configure a community list and route map to match routes with the community attribute of **100:20**.

```
Device A> enable
Device A# configure terminal
Device A(config)# ip community-list standard test permit 100:20
Device A(config)# route-map COM
Device A(config-route-map)# match community test
Device A(config-route-map)# exit
```

(5) On device A, specify the neighbor 192.168.1.2, and use the route map **COM** to filter routes received from the neighbor.

```
Device A(config)# router bgp 100
Device A(config-router)# neighbor 192.168.1.2 route-map COM in
```

5. Verification

Check the community list of device A.

```
Device A> enable
Device A# show ip community-list
Named Community standard list test
permit 100:20
```

Before associating the community list with device A, check the BGP routing table.

```
Device A# show ip bgp
BGP table version is 1, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric     LocPrf     Weight Path
*> 10.0.0.0/24      192.168.1.2            0                    0 200 i
*> 20.0.0.0/24      192.168.1.2            0                    0 200 i
*> 30.0.0.0/24      192.168.1.2            0                    0 200 i
*> 40.0.0.0/24      192.168.1.2            0                    0 200 i

Total number of prefixes 4
```

Check the BGP routes on device A.

```
Device A# show ip bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  200
    192.168.1.2 from 192.168.1.2 (192.168.1.2)
```

```
     Origin IGP, metric 0, localpref 100, valid, external, best
     Community: 100:20 200:20
     Last update: Wed Nov  6 18:58:18 2013
```

After configuring the community list on device A, check the BGP routes to verify that the routes are filtered correctly.

```
Device A# show ip bgp
BGP table version is 1, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric     LocPrf     Weight Path
*> 10.0.0.0/24      192.168.1.2            0                    0 200 i
*> 20.0.0.0/24      192.168.1.2            0                    0 200 i

Total number of prefixes 2
```

6. Configuration Files

- Device A configuration file

```
!
ip community-list standard test permit 100:20
!
route-map COM
 match community test
!
router bgp 100
 neighbor 192.168.1.2 route-map COM in
!
```

- Device B configuration file

```
!
route-map comm1
 set community 100:20 200:20
!
route-map comm2
 set community 100:20
!
route-map comm3
 set community 200:20
!
router bgp 200
 neighbor 192.168.1.1 send-community
 network 10.0.0.0 mask 255.255.255.0 route-map comm1
```

```
 network 20.0.0.0 mask 255.255.255.0 route-map comm2
 network 30.0.0.0 mask 255.255.255.0 route-map comm3
 network 40.0.0.0 mask 255.255.255.0
!
```

Contents

1 Configuring PBR....1
1.1 Introduction....1
1.1.1 Overview....1
1.1.2 Principles....1
1.2 Configuration Task Summary....4
1.3 Configuring Basic Functions of PBR....4
1.3.1 Overview....4
1.3.2 Restrictions and Guidelines....4
1.3.3 Configuration Tasks....4
1.3.4 Applying PBR to an Interface....5
1.3.5 Applying PBR to a Local Device....5
1.4 Configuring Redundant Backup or Load Balancing....6
1.4.1 Overview....6
1.4.2 Restrictions and Guidelines....6
1.4.3 Procedure....7
1.5 Configuring Source-Address-Based PBR....7
1.5.1 Overview....7
1.5.2 Restrictions and Guidelines....7
1.5.3 Procedure....8
1.6 Monitoring....8
1.7 Configuration Examples....10

1.7.1 Configuring PBR to Implement Multi-Exit High Availability.....10

1.7.2 Selecting an Output Link based on Source Addresses of Packets.....14

1 Configuring PBR

1.1 Introduction

1.1.1 Overview

You can apply a route map containing policies to interfaces and devices to implement Policy-Based Routing (PBR).

Similar to static routing, PBR is manually configured and does not automatically update with network changes. It is effective only for packets from local interfaces and devices. PBR is more flexible than static and dynamic routing. Static and dynamic routing forwards packets only based on destination addresses. PBR forwards packets based on the source IP address, destination IP address, packet length, and ingress port.

1.1.2 Principles

1. PBR-Procedure

To implement PBR, perform the following steps:

(1) Define a policy: Use the route map to define matching rules for traffic characteristics and set processing actions.

(2) Apply the policy: Apply the policy to interfaces or local devices.

2. Packet Processing Flow

After the device identifies packets, it processes packets as follows:

(1) Identify the source of traffic to determine the traffic is forwarded or is local, and check whether any policy is applied.

(2) Forward the packets based on the defined policy.

(3) If no next hop is matched or the next hop is unreachable, forward the packets based on the routing table.

(4) If the routing table does not contain any route to the destination address, discard the packets.

3. Definition of a Policy

A policy is a "**match**..., **set**..." statement, which indicates that "if certain conditions are matched, you can perform some processing actions"

Note

For details about the policies, see *Configuring Routing Policies*.

- Executing a policy

  A route map contains multiple policies. Each policy has a sequence number. A smaller sequence number means a higher priority. You can execute policies by sequence number. Once the matching condition of a policy

is met, the processing action of this policy is performed and the route map exits. If no matching condition of any policy is met, no processing is performed.

Policies support two working modes:

- permit: When the matching condition of a policy is met, perform the processing action of this policy and exit the route map.
- deny: When the matching condition of a policy is met, do not perform the processing action of this policy, but exit the route map.

- Matching conditions of policies

  The matching condition of a policy may contain zero, one, or more match rules.

  - If the matching condition contains 0 matching rule, no packet is matched.
  - If the matching condition contains one or more match rules, the matching condition is met only when all the rules are matched.

  In the route map mode, run the **match** command to set matching rules. One **match** command corresponds to one matching rule.

- Processing action for a policy

  The processing action of a policy contains 0, 1 or more set rules.

  - If the processing action contains 0 set rule, no processing action is performed and the route map directly exits.
  - If the processing action contains one or more set rules, all processing actions are performed and then the route map exits.

⚠ Caution

If set rules have different priorities, only the set rule with the highest priority takes effect.

---

4. Application of a Policy

Apply a route map including policies to interfaces or devices to implement PBR.

- If a route map is applied to an interface, packets received by the interface are routed based on the policy.

  The PBR is often used to control user packets received by a device. It is effective only for forwarded packets, but not for locally initiated packets.

- If a route map is applied to a device, locally initiated packets are routed based on the policy.

  The PBR is often used to control protocol packets exchanged between devices (such as ping packets sent locally). It is effective only for locally initiated packets, but not for forwarded packets.

5. Enhanced Reliability of PBR

- Redundant backup or load balancing

You can set multiple next hops in a policy. Either redundant backup or load balancing can be implemented among multiple next hops. Redundant backup is implemented by default.

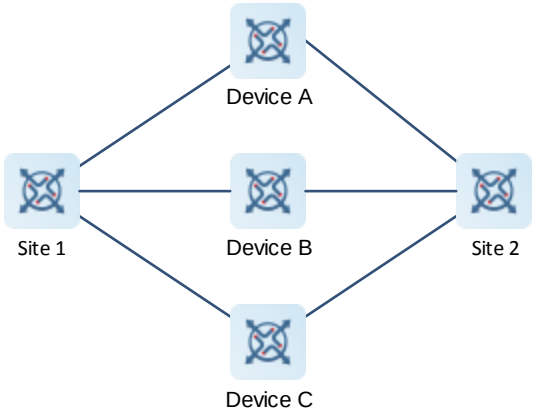
- Redundant backup

  As shown in Figure 1-1, the configuration sequence of the next hop from Site 1 to Site 2 is as follows: Device A > Device B > Device C, and the first accessible next hop takes effect. When the currently effective next hop (Device A) is faulty, the traffic automatically switches to the next accessible next hop (Device B). When Device A becomes accessible again, the traffic automatically switches back to Device A.

  A new next hop stays at the end of the sequence. If the original sequence is Device A > Device B > Device C, and if Device A is added after it is deleted, the current sequence becomes Device B > Device C > Device A.

  If no next hop is accessible, packets are discarded.

Figure 1-1 Redundant backup function



- Load balancing

  When multiple accessible next hops take effect concurrently, the Weighted Cost Multiple Path (WCMP) and Equal Cost Multiple Path (ECMP) are supported. After an accessible next hop fails, traffic will be balanced among the other accessible next hops.

- Correlation with BFD

  Correlation between PBR and BFD helps the PBR to better perceive network environment changes. When BFD finds the current next hop unaccessible, the BFD immediately notifies the PBR of switching the traffic to another accessible next hop (to implement redundant backup) or all the other accessible next hops (to implement load balancing).

- Correlation with Track

  Correlation between PBR and Track helps the PBR to better perceive network environment changes. When Track finds the current next hop unaccessible, the Track immediately notifies the PBR of switching the traffic to another accessible next hop (to implement redundant backup) or all the other accessible next hops (to implement load balancing).

6. Source-address-based PBR

If the source-address-based PBR is generated, you do not need to configure a route map.

- If only the source IPv4 address or source IPv6 address of packets forwarded by the interface needs to be matched, you can run the command of the source-address-based PBR. This command is more simply configured than that of interface-based PBR.
- If the source-address-based PBR is applied to a specified interface, packets received on this interface are routed according to the source addresses.

The PBR is often used to control user packets received by a device. It is effective only for forwarded packets, but not for locally initiated packets.

Note

The source-address-based PBR has a lower priority than the interface-based PBR. If the source-address-based PBR and the interface-based PBR are applied to the same interface, only the interface-based PBR takes effect.

1.2 Configuration Task Summary

The PBR configuration includes the following tasks:

(1) Configuring Basic Functions of PBR

- Applying PBR to an Interface
- Applying PBR to a Local Device

(2) (Optional) Configuring Redundant Backup or Load Balancing

(3) (Optional) Configuring Source-Address-Based PBR

1.3 Configuring Basic Functions of PBR

1.3.1 Overview

This section describes how to perform personalized routing management of user data streams by preparing flexible policies.

1.3.2 Restrictions and Guidelines

- A route map must be used when PBR is configured. Therefore, you must configure a route map on a device.
- If an ACL is used when the route map is configured, you must configure the ACL on the device.
- If the route map used in PBR does not exist, the PBR does not take effect.

1.3.3 Configuration Tasks

The configuration of PBR basic functions includes the following tasks:

- Applying PBR to an Interface
- Applying PBR to a Local Device

1.3.4 Applying PBR to an Interface

1. Overview

This section describes how to apply PBR to an interface to implement personalized routing management on user data streams passing a device.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Apply PBR to IPv4 packets received by an interface.

ip policy route-map *route-map-name*

By default, no PBR is configured on an interface.

(5) Apply PBR to IPv6 packets received by an interface.

ipv6 policy route-map *route-map-name*

By default, no IPv6 PBR is configured on an interface.

1.3.5 Applying PBR to a Local Device

1. Overview

This section describes how to apply PBR to a local device to implement personalized management on packets initiated by the local device. A device has only one IPv4 PBR and one IPv6 PBR.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Apply PBR to IPv4 packets initiated by the local device.

ip local policy route-map *route-map-name*

By default, no IPv4 PBR is applied to the local device.

(4) Apply PBR to IPv6 packets initiated by the local device.

ipv6 local policy route-map *route-map-name*

By default, no IPv6 PBR is applied to the local device.

1.4 Configuring Redundant Backup or Load Balancing

1.4.1 Overview

Multiple next hops in the mutual backup mode can enhance the network reliability.

Load balancing mode among multiple next hops can expand the network bandwidth.

1.4.2 Restrictions and Guidelines

- If redundant backup is selected, the first next hop takes effect based on the configuration sequence.
- If load balancing is selected, all next hops take effect at the same time and share traffic by weight.
- This configuration applies to all PBRs configured on a device.
- The basic functions of PBR must be configured.
- Redundant backup and load balancing are effective only for the next hops set by the following **set** commands, and only among multiple next hops set by the same **set** command.

Table 1-1 set commands for configuring the next hop

Command	Description
set ip next-hop	Configures the next hop of IPv4 packets. This command carries the **weight** parameter to set the weight of the WCMP. The default value is **1**.
set ip default next-hop	Configures the default next hop of IPv4 packets. This command carries the **weight** parameter to set the weight of the WCMP. The default value is 1.
set ipv6 next-hop	Configures the next hop of IPv6 packets. This command carries the **weight** parameter to set the weight of the WCMP. The default value is **1**.
set ipv6 default next-hop	Configures the default next hop of IPv6 packets. This command carries the **weight** parameter to set the weight of the WCMP. The default value is **1**.

Command	Description
set ip next-hop recursive	Configures the recursive next hop of IPv4 packets. Only one command is configured for a route map, and packets can recur to multiple next hops (up to 32 next hops) of a static or dynamic ECMP route. The redundant backup or load balancing mode for recurring to multiple next hops is also determined by the **ip policy** { **redundance** | **load-balance** } command.
set ipv6 next-hop recursive	Configures the recursive next hop of IPv6 packets. Only one command is configured for a route map, and packets can recur to multiple next hops (up to 32 next hops) of a static or dynamic ECMP route. The redundant backup or load balancing mode for recurring to multiple next hops is also determined by the **ipv6 policy** { **redundance** | **load-balance** } command.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an IPv4 PBR to implement redundant backup or load balancing among multiple next hops.

ip policy { **redundance** | **load-balance** }

By default, multiple next hops of the PBR adopt the redundant backup mode.

(4) Configure an **IPv6** PBR to implement redundant backup or load balancing among multiple next hops.

ipv6 policy { **redundance** | **load-balance** }

By default, multiple next hops of the IPv6 PBR adopt the redundant backup mode.

1.5 Configuring Source-Address-Based PBR

1.5.1 Overview

This section describes how to perform personalized routing management for IPv4 or IPv6 addresses of user data streams by preparing flexible policies.

1.5.2 Restrictions and Guidelines

- Source-address-based PBR has a higher priority than interface-based PBR. When they are applied to an interface at the same time, interface-based PBR takes effect whereas source-address-based PBR does not take effect.

- The global configuration takes effect on the input interface of specified user data streams.
- You can specify multiple source-address-based PBRs for the same interface. The sequence numbers of source-address-based PBRs must be different. A smaller sequence number indicates a higher priority of the source-address-based PBR.

  If the sequence number is the same, the priorities of next hop types are as follows:

  next-hop *ip-address* > **default next-hop** *ip-address*

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an **IPv6** PBR to implement redundant backup or load balancing among multiple next hops.

ip policy-source in-interface *interface-type interface-number sequence* { *source-address mask* | *source-address/mask* } { [**default**] **next-hop** [*ipv4-address* [*weight*]]&<1-4> | [**default**] **interface** { *out-interface-type out-interface-number* } &<1-4>}

By default, no source-address-based PBR takes effect on an interface.

(4) Apply a source-address-based PBR for IPv6 packets received by an interface.

ipv6 policy-source in-interface interface-type *interface-number* sequence source-address/prefix-length { [**default**] **next-hop** [ipv6-address [weight]]&<1-4> | [**default**] **interface** out-interface-type&<1-4> }

By default, no source-address-based IPv6 PBR takes effect on an interface.

1.6 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

You can run the **clear** commands to clear information.

Caution

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

You can run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2 Monitoring of the PBR

Command	Purpose
show ip policy [*route-map-name*]	Displays the configurations of the IPv4 PBR.
show ipv6 policy	Displays the configurations of the IPv6 PBR.
show route-map [*name*]	Displays the configurations of a route map.
show access-list	Displays the configurations of an ACL.
show ip pbr bfd	Displays the correlation between the IPv4 PBR and BFD.
show ipv6 pbr bfd	Displays the correlation between the IPv6 PBR and BFD.
show ip pbr route [**interface** *interface-type interface-number* | **local**]	Displays the routing information of the IPv4 PBR.
show ipv6 pbr route [**interface** *interface-type interface-number* | **local**]	Displays the routing information of the IPv6 PBR.
show ip pbr route-map *rmap-name*	Displays a route map used by the IPv4 PBR.
show ipv6 pbr route-map *rmap-name*	Displays a route map used by the IPv6 PBR.
show ip pbr source-route [**interface** *interface-type interface-number*]	Displays the routing information of source-address-based IPv4 PBR.
show ipv6 pbr source-route [**interface** *interface-type interface-number*]	Displays the routing information of source-address-based IPv6 PBR.
show ip pbr statistics [**interface** *interface-type interface-number* | **local**]	Displays the statistics about the IPv4 PBR.
show ipv6 pbr statistics [**interface** *interface-type interface-number* | **local**]	Displays the statistics about the IPv6 PBR.
clear ip pbr statistics [**interface** *interface-type interface-number* | **local**]	Clears the statistics about packets forwarded by the IPv4 PBR.
clear ipv6 pbr statistics [**interface** *interface-type interface-number* | **local**]	Clears the statistics about packets forwarded by the IPv6 PBR.
debug pbr error	Debugs PBR errors.
debug pbr events	Debugs PBR events.

Command	Purpose
debug pbr ms	Debugs multiple service cards supported by PBR.
debug pbr msg	Debugs PBR message communication.
debug pbr nsm	Debugs interaction between PBR and NSM.
debug pbr packet	Debugs packet forwarding of PBR.
debug pbr restart	Debugs PBR GR.

1.7 Configuration Examples

1.7.1 Configuring PBR to Implement Multi-Exit High Availability

1. Requirements

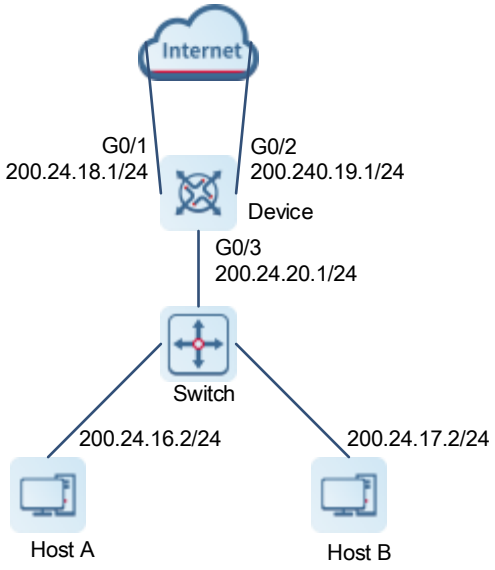
Configure PBR on the devices to achieve the following purposes:

- Packets from Host A (200.24.16.2/24) are sent from GigabitEthernet 0/1 first.
- Packets from Host B (200.24.17.2/24) are sent from GigabitEthernet 0/2 first.

The two output links work in mutual backup mode, and are correlated with Track. Thus, when one link is faulty, traffic is quickly switched over to the other link.

2. Topology

Figure 1-2 PBR topology



3. Notes

- Configure two different ACLs to match packets in the Host A and Host B network segment respectively.
- Configure the route map RM_FOR_PBR: policy 10 is used to ensure that "packets in the Host A network segment are sent from GigabitEthernet 0/1first"; policy 20 is used to ensure that "packets in the Host B network segment are sent from GigabitEthernet 0/2 first".
- Configure a PBR to implement redundant backup among multiple next hops.
- Configure the track rules and correlation between PBR and Track.
- Configure PBR and apply the route map RM_FOR_PBR to packets received from GigabitEthernet 0/3.

4. Procedure

(1) Configure the IP addresses of interfaces to implement interworking between networks. (Omitted)

(2) Configure ACLs for subnets 200.24.16.0/24 and 200.24.17.0/24, respectively.

```
Device> enable
Device# configure terminal
Device(config)# access-list 1 permit 200.24.16.0 0.0.0.255
Device(config)# access-list 2 permit 200.24.17.0 0.0.0.255
```

(3) Configure the track rules.

```
Device(config)# ip rns 1
Device(config-ip-rns)# icmp-echo 200.24.18.1
Device(config-ip-rns)# exit
Device(config)# ip rns schedule 1 start-time now life forever
Device(config)# track 1 rns 1
Device(config)# ip rns 2
Device(config-ip-rns)# icmp-echo 200.24.19.1
Device(config-ip-rns)# exit
Device(config)# ip rns schedule 2 start-time now life forever
Device(config)# track 2 rns 2
```

(4) Configure the PBR **RM_FOR_PBR**, set the next hop of 200.24.16.0 to **200.24.18.1** and its backup next hop to **200.24.19.1**, and set the next hop of 200.24.17.0 to **200.24.19.1** and its backup next hop to **200.24.18.1**.

```
Device(config)# route-map RM_FOR_PBR 10
Device(config-route-map)# match ip address 1
Device(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1
Device(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track 2
Device(config-route-map)# exit
Device(config)# route-map RM_FOR_PBR 20
Device(config-route-map)# match ip address 2
Device(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track 2
Device(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1
Device(config-route-map)# exit
```

(5) Apply the route map RM_FOR_PBR to GigabitEthernet 0/3, and enable load balancing.

```
Device(config)# interface GigabitEthernet 0/3
Device(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR
Device(config-if-GigabitEthernet 0/3)# exit
Device(config)# ip policy redundance
```

5. Verification

Check the PBR configurations to verify that the route map is applied to the interface.

```
Device# show ip policy
Balance mode: redundance
Interface                          Route map
GigabitEthernet 0/3                  RM_FOR_PBR
!
```

Check the configurations of the route map to verify the policy rules.

```
Device# show route-map
route-map RM_FOR_PBR, permit, sequence 10
  Match clauses:
    ip address 1
  Set clauses:
    ip next-hop 200.24.18.1
    ip next-hop 200.24.19.1
route-map RM_FOR_PBR, permit, sequence 20
  Match clauses:
    ip address 2
  Set clauses:
    ip next-hop 200.24.19.1
    ip next-hop 200.24.18.1
```

Check the ACL configurations to verify the packet filtering rules.

```
Device# show access-lists
ip access-list standard 1
 10 permit 200.24.16.0 0.0.0.255
 10 permit 200.24.16.0 0.0.0.255
ip access-list standard 2
 10 permit 200.24.17.0 0.0.0.255
```

Check whether the track objects are up.

```
Device#show track
Track 1
  Reliable Network Service 1
  The state is Up
    1 change, current state last: 120 secs
  Delay up 30 secs, down 50 secs
```

```
Track 2
  Reliable Network Service 2
  The state is Up
    1 change, current state last: 130 secs
  Delay up 30 secs, down 50 secs
```

6. Configuration Files

Device configuration file

```
!
ip policy redundance
!
access-list 1 permit 200.24.16.0 0.0.0.255
access-list 2 permit 200.24.17.0 0.0.0.255
!
route-map RM_FOR_PBR 10
 match ip address 1
 set ip next-hop verify-availability 200.24.18.1 track 1
 set ip next-hop verify-availability 200.24.19.1 track 2
!
route-map RM_FOR_PBR 20
 match ip address 2
 set ip next-hop verify-availability 200.24.19.1 track 2
 set ip next-hop verify-availability 200.24.18.1 track 1
!
ip rns 1
 icmp-echo 200.24.18.1
!
ip rns 2
 icmp-echo 200.24.19.1
!
ip rns schedule 1 start-time now life forever
ip rns schedule 2 start-time now life forever
!
track 1 rns 1
!
track 2 rns 2
!
interface GigabitEthernet 0/3
 ip policy route-map RM_FOR_PBR
!
```

7. Common Errors

- After matching of ACLs and prefix-lists is configured, the corresponding ACLs and prefix lists are not defined.

1.7.2 Selecting an Output Link based on Source Addresses of Packets

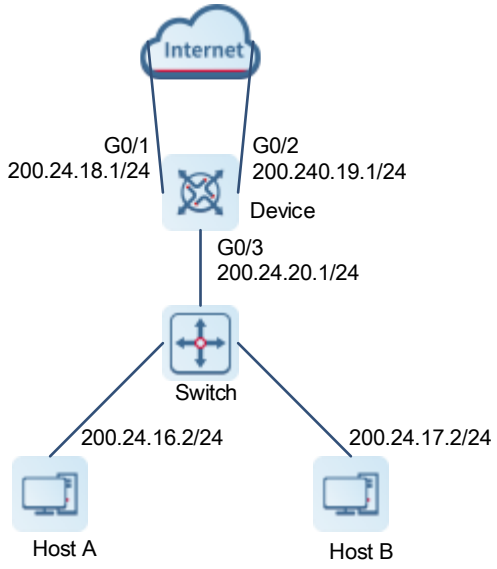
1. Requirements

This LAN has two output interfaces for connecting the Internet. The requirements are as follows:

- Route the Internet access data streams from Host A to GigabitEthernet 0/1.
- Route the Internet access data streams from Host B to GigabitEthernet 0/2.
- If the link on GigabitEthernet 0/1 is disconnected, switch over the data streams from GigabitEthernet 0/1 to GigabitEthernet 0/2. Vice versa.

2. Topology

Figure 1-3 Topology for selecting an output link based on source addresses of packets



3. Notes

- Configure a source-address-based PBR, and set the next hops for packets from the GigabitEthernet 0/3 of Host A to **GigabitEthernet 0/1** and **GigabitEthernet 0/2**. (Note the configuration sequence.)
- Configure a source-address-based PBR, and set the next hops for packets from the GigabitEthernet 0/3 of Host B to **GigabitEthernet 0/2** and **GigabitEthernet 0/1**. (Note the configuration sequence.)
- Configure a PBR to implement redundant backup among multiple next hops. (The default setting is redundant backup.)

4. Procedure

(1) Configure basic networks, such as the interface IP address.

(2) Select an output link based on source addresses of packets.

```
Device> enable
Device# configure terminal
Device (config)# ip policy-source in-interface gigabitEthernet 0/3 1 200.24.16.0/24
next-hop 200.24.18.1 200.24.19.1
Device (config)# ip policy-source in-interface gigabitEthernet 0/3 2 200.24.17.0/24
next-hop 200.24.19.1 200.24.18.1
Device (config)# ip policy redundance
```

5. Verification

Check the configurations of the source-address-based IPv4 PBR.

```
Device # show ip pbr source-route
PBR IPv4 Source Route
Interface       : GigabitEthernet 0/3
  Sequence      : 1
  Source address : 200.24.16.0/24
  VRF ID        : 0
  Route Flags    :
   Route Type    : PBR
   Direct       : Permit
   Priority     : High
   Match_ipaddr  : Exist
  Mode          : redundance
  Nexthop Count  : 2
   Nexthop[0]    : 200.24.18.1
   Weight[0]     : 1
   Ifindex[0]    : 1
   Nexthop[1]    : 200.24.19.1
   Weight[1]     : 1
   Ifindex[1]    : 2

Interface       : GigabitEthernet 0/3
  Sequence      : 2
  Source address : 200.24.17.0/24
  VRF ID        : 0
  Route Flags    :
   Route Type    : PBR
   Direct       : Permit
   Priority     : High
   Match_ipaddr  : Exist
  Mode          : redundance
  Nexthop Count  : 2
   Nexthop[0]    : 200.24.19.1
```

```
  Weight[0]    : 1
  Ifindex[0]   : 2
  Nexthop[1]   : 200.24.18.1
  Weight[1]    : 1
  Ifindex[1]   : 1
```

6. Configuration Files

Device configuration file

```
!
ip policy-source in-interface gigabitEthernet 0/3 1 200.24.16.0/24 next-hop 200.24.18.1
200.24.19.1
ip policy-source in-interface gigabitEthernet 0/3 2 200.24.17.0/24 next-hop 200.24.19.1
200.24.18.1
ip policy redundance
!
```

Contents

1 Configuring Keys 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Configuring a Key Chain 1
1.2.1 Overview 1
1.2.2 Restrictions and Guidelines 1
1.2.3 Configuration Tasks 2
1.2.4 Creating a Key Chain 2
1.2.5 Configuring a Key ID 2
1.2.6 Configuring a Key String 3
1.2.7 Configuring the Send-Lifetime 4
1.2.8 Configuring the Accept-Lifetime 4
1.3 Monitoring 5
1.4 Configuration Examples 5
1.4.1 Configuring a Key Chain and Using the Key Chain in RIP Packet Authentication 5

1 Configuring Keys

1.1 Introduction

1.1.1 Overview

Keys are a kind of parameters that are used in algorithms for conversion from plaintext to ciphertext or from ciphertext to plaintext.

To allow packet authentication in a routing protocol to support plaintext authentication and ciphertext authentication, you must use keys.

Note

- Now, keys are used only for RIP and ISIS packet authentication.
- In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be Layer-3 switches, routers, or firewalls.

1.1.2 Principles

The key chain provides a tool for the authentication mechanism in a routing protocol.

1. Key Chain

A key chain contains the TCP authentication configuration, authentication algorithm ID, and multiple different keys. Each key has the following attributes:

- Key ID: Identifies a key. In the current key chain, each key corresponds to one ID.
- Authentication string: Specifies a set of key characters used for verifying the consistency of authentication strings in a routing protocol.
- Lifetime: Specifies the lifetime of the current key for sending or receiving packets. Different authentication keys can be used in different periods.
- Authentication algorithm: It is used by keys to authenticate routing protocols.

1.2 Configuring a Key Chain

1.2.1 Overview

This section defines a key chain to be used by a routing protocol.

1.2.2 Restrictions and Guidelines

A key chain can take effect only after it is associated with a routing protocol.

1.2.3 Configuration Tasks

The key configuration includes the following tasks:

(1) Creating a Key Chain

(2) Configuring a Key ID

(3) Configuring a Key String

(4) (Optional) Configuring the Send-Lifetime

(5) (Optional) Configuring the Accept-Lifetime

1.2.4 Creating a Key Chain

1. Overview

In the global configuration mode, you can run the **key chain** *key-chain-name* command to define a key chain and enter the key chain configuration mode.

2. Restrictions and Guidelines

- This configuration is mandatory if a key chain needs to be used.
- If there is no special requirement, you should perform this configuration on all routers that need to authenticate routing protocols.
- To make a key chain take effect, you must configure at least one key.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a key chain, and enter the key chain configuration mode.

key chain *key-chain-name*

No key chain is configured by default.

1.2.5 Configuring a Key ID

1. Overview

In the key chain configuration mode, you can run the **key** *key-id* command to define a key and enter the key chain key configuration mode.

2. Restrictions and Guidelines

- This configuration is mandatory if a key chain needs to be used.

- If there is no special requirement, you should perform this configuration on all devices that need to authenticate routing protocols.
- After the key is configured, it must meet two conditions before it takes effect: (1) the key-string is configured; (2) the key is in the lifetime (send-lifetime and accept-lifetime). If the lifetime is not configured, the key is considered effective permanently once the key-string is configured. Two effective states are defined: effective on the sending end and effective on the receiving end. The two states correspond to send-lifetime and accept-lifetime respectively.
- If there is no special demand, you can configure a key by incrementing the key-id to avoid the authentication state oscillation caused by the possible changes of effective keys. If multiple effective keys exist, each routing protocol uses the key with the smallest key-id.
- In the TCP enhanced authentication scenario, the key-id ranges from 0 to 63.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the key chain configuration mode.

key chain *key-chain-name*

(4) Create a key ID, and enter the key configuration mode of the key chain.

key *key-id*

No key is configured by default.

1.2.6 Configuring a Key String

1. Overview

In the key configuration mode of the key chain, you can specify a key string in plaintext or cyphertext. To ensure security, you are advised to use cyphertext. If you run the **service password-encryption** command to enable the encryption service, you can forcibly convert a plaintext key string into a ciphertext string.

2. Restrictions and Guidelines

- This configuration is mandatory if a key chain needs to be used.
- If there is no special requirement, you should perform this configuration on all routers that need to authenticate routing protocols.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the key chain configuration mode.

key chain *key-chain-name*

(4) Enter the key configuration mode of the key chain.

key *key-id*

(5) Configure a key string.

key-string [**0 | 7**] *string-text*

No key string is configured by default.

1.2.7 Configuring the Send-Lifetime

1. Overview

This section defines the lifetime of a key in the sending direction.

2. Restrictions and Guidelines

If the send-lifetime is not configured, the key chain is always effective.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the key chain configuration mode.

key chain *key-chain-name*

(4) Enter the key configuration mode of the key chain.

key *key-id*

(5) Configure the send-lifetime.

send-lifetime *start-time* { **infinite** | *end-time* | **duration** *duration-time* }

By default, the send-lifetime of a key chain is disabled.

1.2.8 Configuring the Accept-Lifetime

1. Overview

This section defines the lifetime of a key in the receiving direction.

2. Restrictions and Guidelines

If the accept-lifetime is not configured, the key chain is always effective.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the key chain configuration mode.

key chain *key-chain-name*

(4) Enter the key configuration mode of the key chain.

key *key-id*

(5) Configure the accept-lifetime.

accept-lifetime *start-time* { **infinite** | *end-time* | **duration** *duration-time* }

By default, the accept-lifetime of a key chain is disabled.

1.3 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Key Monitoring

Command	Purpose
show key chain [*key-chain-name*]	Displays the configurations of a key chain.

1.4 Configuration Examples

1.4.1 Configuring a Key Chain and Using the Key Chain in RIP Packet Authentication

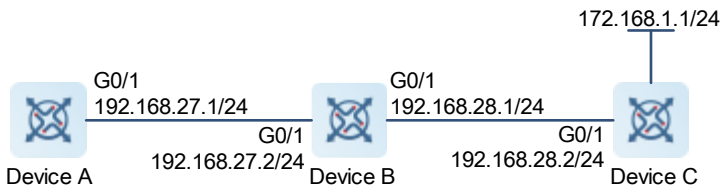
1. Requirements

Device A and Device B are interconnected using the RIP routing protocol. To improve security, you can configure the MD5 encryption algorithm between Device A and Device B to encrypt RIP packets.

Device B accesses 172.168.1.1/24 via the static route.

2. Topology

Figure 1-1 Topology for key authentication



3. Notes

- Configure keys on all routers.
- Configure RIP on all routers.
- Enable RIP authentication on all routers.

4. Procedure

(1) Configure the IP addresses of interfaces.

Configure Device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitEthernet 0/1
Device A(config-if)# ip address 192.168.27.1 255.255.255.0
Device A(config-if)# exit
```

Configure Device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface gigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.27.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# exit
```

(2) Configure keys and lifetime of each key.

Configure Device A.

```
Device A# configure terminal
Device A(config)# key chain ripchain
Device A(config-keychain)# key 1
Device A(config-keychain-key)# key-string Hello
Device A(config-keychain-key)# accept-lifetime 16:30:00 Oct 1 2013 duration 43200
Device A(config-keychain-key)# send-lifetime 16:30:00 Oct 1 2013 duration 43200
Device A(config-keychain-key)# exit
Device A(config-keychain)# key 2
```

```
Device A(config-keychain-key)# key-string World
Device A(config-keychain-key)# accept-lifetime 04:00:00 Oct 2 2013 infinite
Device A(config-keychain-key)# send-lifetime 04:00:00 Oct 2 2013 infinite
Device A(config-keychain-key)# exit
```

Configure Device B.

```
Device B# configure terminal
Device B(config)# key chain ripchain
Device B(config-keychain)# key 1
Device B(config-keychain-key)# key-string Hello
Device B(config-keychain-key)# accept-lifetime 16:30:00 Oct 1 2013 duration 43200
Device B(config-keychain-key)# send-lifetime 16:30:00 Oct 1 2013 duration 43200
Device B(config-keychain-key)# exit
Device B(config-keychain)# key 2
Device B(config-keychain-key)# key-string World
Device B(config-keychain-key)# accept-lifetime 04:00:00 Oct 2 2013 infinite
Device B(config-keychain-key)# send-lifetime 04:00:00 Oct 2 2013 infinite
Device B(config-keychain-key)# exit
```

(3) Configure the basic RIP.

Configure Device A.

```
Device A(config)# router rip
Device A(config-router)# version 2
Device A(config-router)# network 192.168.27.0
Device A(config-router)# exit
```

Configure Device B.

```
Device B(config)# router rip
Device B(config-router)# version 2
Device B(config-router)# network 192.168.27.0
Device B(config-router)# redistribute static
Device B(config-router)# exit
```

(4) Set the interface authentication mode to MD5, and specify the authentication key chain.

Configure Device A.

```
Device A(config)# interface gigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain ripchain
Device A(config-if)# ip rip authentication mode md5
```

Configure Device B.

```
Device B(config)# interface gigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip address 192.168.27.2 255.255.255.0
Device B(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain ripchain
Device B(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5
```

5. Verification

Check whether Device A can receive routes from Device B.

```
Device A# show ip route rip
R    172.168.0.0/16 [120/1] via 192.168.27.2, 00:05:16, GigabitEthernet 0/1
```

6. Configuration Files

- Device A configuration file

```
!
key chain ripchain
 key 1
  key-string Hello
  accept-lifetime 16:30:00 Oct 1 2013 duration 43200
  send-lifetime 16:30:00 Oct 1 2013 duration 43200
 key 2
  key-string World
  accept-lifetime 04:00:00 Oct 2 2013 infinite
  send-lifetime 04:00:00 Oct 2 2013 infinite
!
interface gigabitEthernet 0/1
 ip address 192.168.27.1 255.255.255.0
 ip rip authentication key-chain ripchain
 ip rip authentication mode md5
!
router rip
 version 2
 network 192.168.27.0
!
```

- Device B configuration file

```
!
key chain ripchain
 key 1
  key-string Hello
  accept-lifetime 16:30:00 Oct 1 2013 duration 43200
  send-lifetime 16:30:00 Oct 1 2013 duration 43200
key 2
  key-string World
  accept-lifetime 04:00:00 Oct 2 2013 infinite
  send-lifetime 04:00:00 Oct 2 2013 infinite
!
interface gigabitEthernet 0/1
 ip address 192.168.27.2 255.255.255.0
```

```
 ip rip authentication key-chain ripchain
 ip rip authentication mode md5
!
router rip
 version 2
 network 192.168.27.0
 redistribute static
!
```

7. Common Errors

- A key is not correctly associated with a routing protocol, resulting in authentication failures.
- The keys configured on multiple routers are inconsistent, resulting in authentication failures.

Multicast Configuration

1. IPv4 Multicast Configuration
2. IGMP Configuration
3. PIM-SM Configuration
4. PIM-DM Configuration
5. IGMP Snooping Configuration
6. MSDP Configuration
7. IPv6 Multicast Configuration
8. MLD Configuration
9. PIM-SMv6 Configuration
10. MLD Snooping Configuration

Contents

1 Configuring Multicast Basics 1

1.1 Basic Concepts of Multicast 1

1.2 Multicast Service Models 2

1.2.1 ASM Model 2

1.2.2 SSM Model 2

1.3 Multicast Address 2

1.3.1 IPv4 Multicast Address 2

1.3.2 IPv4 Multicast MAC Address 3

1.3.3 IPv6 Multicast Address 4

1.3.4 IPv6 Multicast MAC Address 5

1.4 IPv4 Multicast Protocols 5

1.5 IPv6 Multicast Protocols 6

1.6 Basic Concepts of PIM 7

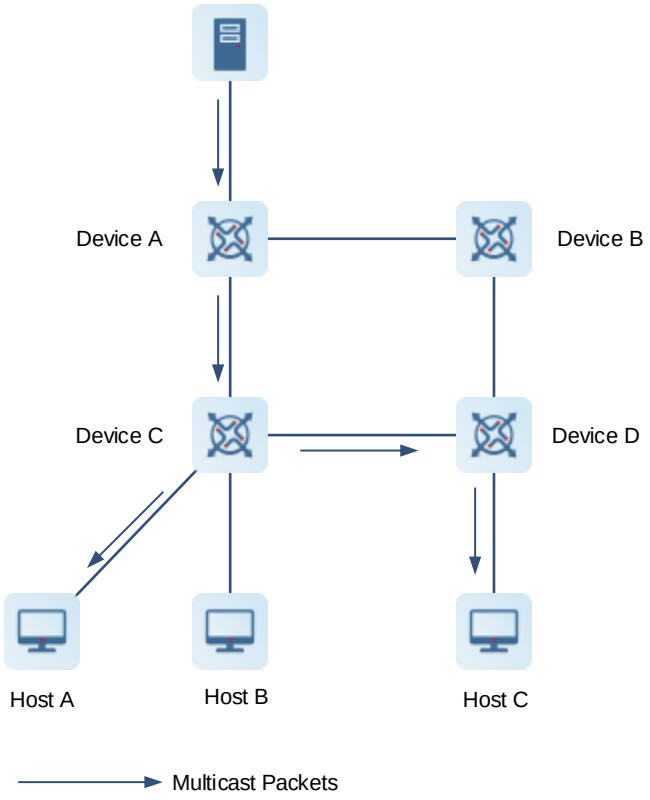
1 Configuring Multicast Basics

IP transmission methods are categorized into unicast, multicast, and broadcast. In IP multicast, an IP packet is sent from a source and forwarded to a specific group of receivers. Compared with unicast and broadcast, IP multicast saves bandwidth and reduces network loads. Therefore, IP multicast is applied to different network services that have high requirements for real timeliness, for example, Internet TV, distance education, live broadcast and multimedia conference.

1.1 Basic Concepts of Multicast

As shown in Figure 1-1, there are packet sending sources and receivers on a network. Users who are interested in information raise information requirements. Then, the information sending source sends information only to these users.

Figure 1-1 Topology of Multicast Data Transmission



- Multicast group: It is marked based on a multicast IP address. After a host is added to a multicast group, the host becomes a member of the multicast group and can receive multicast packets destined to the multicast group.
- Multicast source: Indicates a packet sender, for example, the source in Figure 1-1. Different multicast sources can send packets to a multicast group, and a multicast source can send multicast packets to different multicast groups.
- Member of multicast group: Indicates a host that is added to a multicast group, for example, Host A and Host

C in Figure 1-1. Members in a multicast group can be dynamically added to or removed from the multicast group.

- Multicast device: Indicates a router or switch that supports the multicast function. For example, the devices in Figure 1-1 can provide multicast routing and member management functions.

1.2 Multicast Service Models

Based on members in a multicast group, the service models of multicast can be categorized into Any-Source Multicast (ASM) and Source-Specific Multicast (SSM). The two service models use different address ranges of multicast groups.

1.2.1 ASM Model

In the ASM model, multicast data is assigned to multicast groups. The address of a multicast group is used as a network service ID. Any multicast source can send packets to this multicast group, and hosts join the group to receive multicast packets from this multicast group. The address of the multicast group in the ASM model is unique on the multicast network.

1.2.2 SSM Model

In the SSM model, multicast data is assigned to specific multicast sources and multicast groups. When you add a host to a multicast group, you can configure it to receive or not receive data from the specified multicast sources After the host is added to the multicast group, the host can receive only multicast data that is sent to this multicast group by the specified multicast sources. In the SSM model, different multicast sources can use the same address of a multicast group.

1.3 Multicast Address

The multicast technology provides network layer multicast for communication between a multicast source and members in a multicast group based on a multicast IP address. The multicast technology ensures transmission of multicast data in a local physical network based on a multicast MAC address. The IP address must be mapped to the MAC address to ensure correct transmission of the multicast data, because the members in the multicast group are unknown.

1.3.1 IPv4 Multicast Address

The four higher-order bits of a class D IP address are 1110, and the IP address range is from 224.0.0.0 to 239.255.255.255. These four bits are assigned by the Internet Assigned Numbers Authority (IANA) to IPv4 multicast. Table 1-1 lists how IPv4 multicast addresses are allocated.

Table 1-1 Assignment of IPv4 Multicast Addresses

Address Range	Description
224.0.0.0~224.0.0.255	Address of a permanent group
224.0.1.0~231.255.255.255 233.0.0.0~238.255.255.255	ASM multicast address
232.0.0.0~232.255.255.255	Default SSM multicast address

Address Range	Description
239.0.0.0~239.255.255.255	Address of a local management group

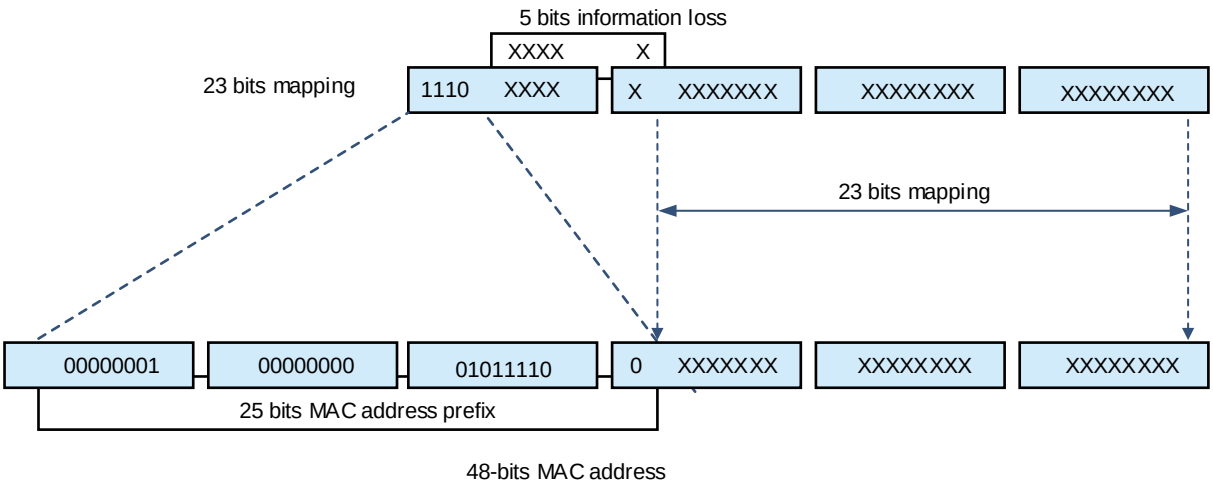
Table 1-2 Addresses of Common Permanent Groups

Address of a Permanent Group	Description
224.0.0.0	Unallocated
224.0.0.1	All hosts and routers in a network segment
224.0.0.2	All multicast devices
224.0.0.3	Unallocated
224.0.0.4	Distance Vector Multicast Routing Protocol (DVMRP) router
224.0.0.5	Open Shortest Path First (OSPF) router
224.0.0.6	OSPF specified router
224.0.0.7	Shared tree (ST) router
224.0.0.8	ST host
224.0.0.9	Routing Information Protocol version 2 (RIP-2) router
224.0.0.11	Mobile proxy
224.0.0.12	Dynamic Host Configuration Protocol (DHCP) server/relay proxy
224.0.0.13	All Protocol Independent Multicast (PIM) devices
224.0.0.14	Resource Reservation Protocol (RRP) encapsulation
224.0.0.15	All Core-Based Tree (CBT) routers
224.0.0.16	Specified Subnetwork Bandwidth Management (SBM)
224.0.0.17	All SBMs
224.0.0.18	Virtual Router Redundancy Protocol (VRRP)

1.3.2 IPv4 Multicast MAC Address

Based on IANA regulation, the higher-order 24 bits of an IPv4 multicast MAC address is 0x01005e, the 25th bit is 0, and the lower-order 23 bits are those of the IPv4 multicast address. Figure 1-2 shows the mapping. The four higher-order bits of an IPv4 multicast address is fixed at 1110, corresponding to the higher-order 25 bits of the MAC address. The lower-order 23 bits in the later 28 bits of the IPv4 multicast address map to the lower-order bits of the multicast MAC address. The lost information indicating by five bits causes the 32 IPv4 addresses to map to the same MAC address.

Figure 1-2 Mapping of IPv4 Multicast Address to IPv4 Multicast MAC Address



1.3.3 IPv6 Multicast Address

An IPv6 address consists of 128 bits. An IPv6 multicast address always starts with FF.

Table 1-3 Assignment of IPv6 Multicast Addresses

Address Range	Description
FF0x::/32	Addresses of a reserved group
FF1x::/32 (x cannot be 1 or 2) FF2x::/32 (x cannot be 1 or 2)	ASM multicast address
FF3x::/32 (x cannot be 1 or 2)	Default SSM multicast address

Table 1-4 Common IPv6 Multicast Addresses and Description

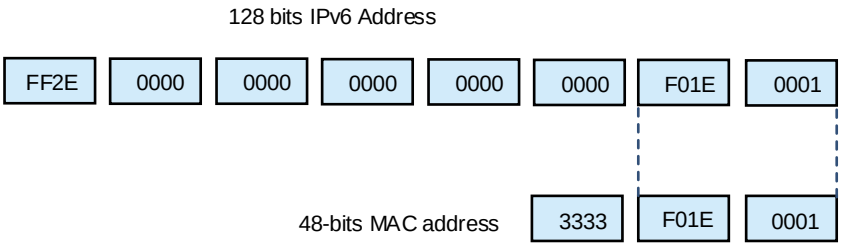
Range	IPv6 Multicast Address	Description
Local range of a node (or an interface)	FF01::1	Addresses of all nodes (interfaces)
	FF01::2	Addresses of all routers
Local range of a link	FF02::1	Addresses of all nodes
	FF02::2	Addresses of all routers
	FF02::3	Unallocated
	FF02::4	DVMRP router
	FF02::5	OSPF IGP router
	FF02::6	OSPF IGP DR

Range	IPv6 Multicast Address	Description
	FF02::7	ST router
	FF02::8	ST host
	FF02::9	RIP router
	FF02::A	EIGRP router
	FF02::B	Mobile proxy
	FF02::D	All PIM routers
	FF02::E	RSVP encapsulation
	FF02::1:1	Link name
	FF02::1:2	All DHCP proxies
	FF02::1:FFXX:XXXX	Solicited-Node address. XX:XXXX indicates the lower-order 24 bits of an IPv6 address of a node.
Local range of station	FF05::2	Addresses of all routers
	FF05::1:3	All DHCP servers
	FF05::1:4	All DHCP relays
	FF05::1:1000~FF05::1:13FF	Service location

1.3.4 IPv6 Multicast MAC Address

The higher-order 16 bits of an IPv6 multicast MAC address is 0x3333, and the lower-order 32 bits are those of the IPv6 multicast address. Figure 1-3 shows the mapping of the IPv6 multicast address FF2E::F01E:1 to the MAC address. There are more IPv6 multicast addresses mapped to the same MAC address.

Figure 1-3 Mapping of IPv6 Address to Multicast MAC Address



1.4 IPv4 Multicast Protocols

A complete set of protocols is developed during the development of multicast to complete multicast data transmission. IPv4 multicast covers the following protocols:

- Internet Group Management Protocol (IGMP): Manages IPv4 multicast members and runs in the network segment that hosts are connected to. IGMP supports data communication with the upstream multicast routing protocols, and maintains and manages relationship of members by adding or removing the members. Three versions of IGMP are available:
  - IGMPv1: Supports the ASM model, and supports the SSM model only when SSM mapping is configured.
  - IGMPv2: Supports the ASM model, and supports the SSM model only when SSM mapping is configured.
  - IGMPv3: Supports the ASM and SSM models.
- PIM: It is a multicast routing protocol in an IPv4 network, and used for route-based query and forwarding of multicast data. PIM includes the following two types:
  - Protocol Independent Multicast Dense Mode (PIM-DM): Applies to a small-size network in which members of a multicast group are densely distributed. The protocol is not distinguished in the ASM and SSM models.
  - Protocol Independent Multicast Sparse Mode (PIM-SM): Applies to a network in any form, and especially applies to a large-size network in which members of a multicast group are sparsely distributed. The protocol is distinguished in the ASM and SSM models based on the data and the multicast addresses in protocol packets.
- Internet Group Management Protocol Snooping (IGMP Snooping): Creates a multicast L2 forwarding table by listening to the IGMP packets between upstream L3 devices and member hosts, and manages and controls multicast packet forwarding on L2 network to suppress multicast data flooding.
- Multicast Source Discovery Protocol (MSDP): Connects multiple PIM-SM domains, shares multicast sources among the PIM-SM domains, and forwards multicast packets across the domains.

1.5 IPv6 Multicast Protocols

IPv6 multicast covers the following protocols:

- Multicast Listener Discovery (MLD): Manages IPv6 multicast members and runs in the network segment that hosts are connected to. MLD supports data communication with the upstream multicast routing protocols, and maintains and manages relationship of members by adding or removing the members. Two versions of MLD are available:
  - MLDv1: Supports the ASM model, and supports the SSM model only when SSM mapping is configured.
  - MLDv2: Supports the ASM and SSM models.
- PIM (IPv6): It is a multicast routing protocol in an IPv6 network, and used for route-based query and forwarding of multicast data. This protocol applies to a network in any form, and especially applies to a large-size network in which members of a multicast group are sparsely distributed. The protocol is distinguished in the ASM and SSM models based on the data and the multicast addresses in protocol packets.
- Multicast Listener Discovery Snooping (MLD Snooping): Creates a multicast L2 forwarding table by listening to the MLD packets between upstream L3 devices and member hosts, and manages and controls multicast packet forwarding on L2 network to suppress multicast data flooding.

1.6 Basic Concepts of PIM

- PIM device

  A device on which PIM is enabled. Multicast packets are forwarded on the PIM device.

- PIM interface

  An interface on which PIM is enabled. The PIM interface that receives multicast packets is an upstream interface, and the PIM interface that sends multicast packets is a downstream interface. The network segment where the upstream interface resides is an upstream network segment, and the network segment where the downstream interface resides is a downstream network segment.

- PIM network

  Connections of PIM devices through the PIM interfaces constitute a PIM network.

- PIM domain

  On some PIM interfaces, borders can be set to divide a large PIM network into multiple PIM domains. The borders can reject specified multicast packets or control transmission of PIM messages.

- Rendezvous point (RP)

  A PIM device functioning as an RP collects multicast source and group member information on a network.

- Candidate-RP (C-RP)

  A device selects RPs from C-RPs based on the election mechanism, and enables the RPs to serve different multicast groups.

- Designated router (DR)

  A PIM device can function as a DR. A DR that is connected to a multicast source and reports multicast source information to the RP is referred to as a source DR. A DR that is connected to members of a multicast group and reports the group member information to the RP is referred to as a member DR.

- Candidate-BSR (C-BSR)

  PIM devices can be configured as C-BSRs, from which a BSR is elected. When the BSR becomes faulty, other C-BSRs initiate a new election request to elect a new BSR. This avoids service interruption.

- Bootstrap router (BSR)

  A PIM device functioning as a BSR collects and releases RP information in a PIM-SM domain. A BSR is elected from candidate-BSRs. Only one BSR is available in a PIM-SM domain. However, there can be multiple candidate-BSRs in the PIM-SM domain.

- Multicast distribution tree

  Multicast packets are transmitted from one point to multiple points. The forwarding path is displayed as a tree. This forwarding path is referred to as a multicast distribution tree (MDT). There are two types of MDTs:

  - RP tree (RPT): The RP is regarded as the root, and the DRs that connect group members are regarded as leaves.
  - Shortest path tree (SPT): The DR that connects multicast sources is regarded as the root, and the RPs or DRs that connect group members are regarded as leaves.

- (*, G) and (S, G)

  - (*, G) refers to a routing entry corresponding to packets that are sent from any multicast source to Group G. The forwarding path corresponding to the packets that are sent from any multicast source to Group G

is referred to as an RPT.

- (S, G) refers to a routing entry corresponding to packets that are sent from source S to Group G. The forwarding path corresponding to the packets that are sent from source S to Group G is an SPT.

Contents

1 Configuring IPv4 Multicast Route Management 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Basic Topology of IPv4 Multicast 1
1.1.3 Basic Concepts of IPv4 Multicast 2
1.1.4 Principle of IPv4 Multicast Forwarding 3
1.1.5 RPF Checking 3
1.1.6 RPF Checking and Multicast Packet Forwarding 5
1.2 Restrictions and Guidelines 5
1.3 Configuration Task Summary 5
1.4 Configuring Basic Functions of IPv4 Multicast 6
1.4.1 Overview 6
1.4.2 Restrictions and Guidelines 6
1.4.3 Procedure 6
1.5 Configuring RPF Route Selection Based on the Longest Match Rule 7
1.5.1 Overview 7
1.5.2 Restrictions and Guidelines 7
1.5.3 Procedure 7
1.6 Configuring Static Routes of IPv4 Multicast 7
1.6.1 Overview 7
1.6.2 Procedure 7
1.7 Configuring IPv4 Multicast Borders 8

1.7.1 Overview 8

1.7.2 Restrictions and Guidelines 8

1.7.3 Procedure 8

1.8 Configuring L2 Direction Control for Multicast Streams 8

1.8.1 Overview 8

1.8.2 Restrictions and Guidelines 9

1.8.3 Procedure 9

1.9 Configuring TTL Threshold 9

1.9.1 Overview 9

1.9.2 Restrictions and Guidelines 9

1.9.3 Procedure 9

1.10 Configuring Forced Forwarding of Multicast Packets by Software 10

1.10.1 Overview 10

1.10.2 Procedure 10

1.11 Configuring Entry Capacity of IPv4 Multicast Routing Table 10

1.11.1 Overview 10

1.11.2 Procedure 10

1.12 Configuring the Overwriting Mechanism upon Overflow of Multicast Hardware Forwarding Entries 11

1.12.1 Overview 11

1.12.2 Procedure 11

1.13 Configuring Multicast Non-Stop Forwarding Parameters 11

1.13.1 Overview 11

1.13.2 Procedure 11

1.14 Monitoring 12

1.15 Common Misconfigurations 13

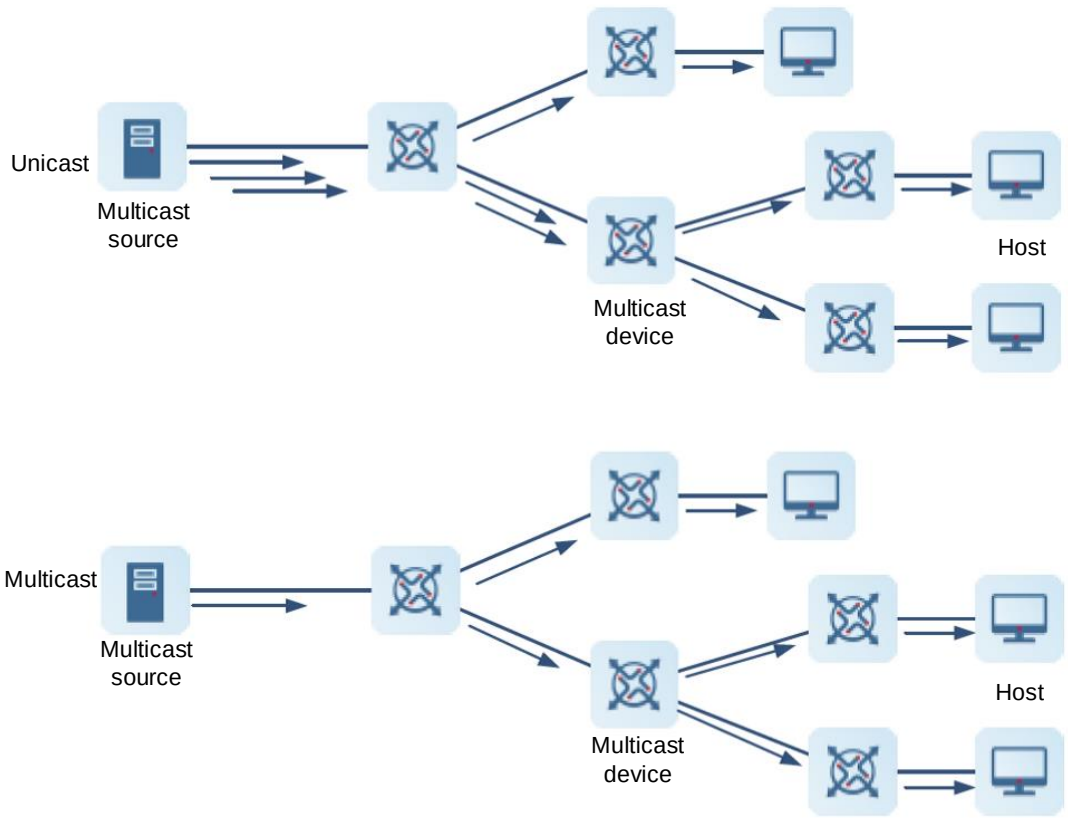
1 Configuring IPv4 Multicast Route Management

1.1 Introduction

1.1.1 Overview

IPv4 multicast transmits a packet from a source to multiple devices. The multicast packet is sent from the source, forwarded by intermediate devices, and then received by receivers in a specified group.

Figure 1-1 Multicast Topology vs. Unicast Topology



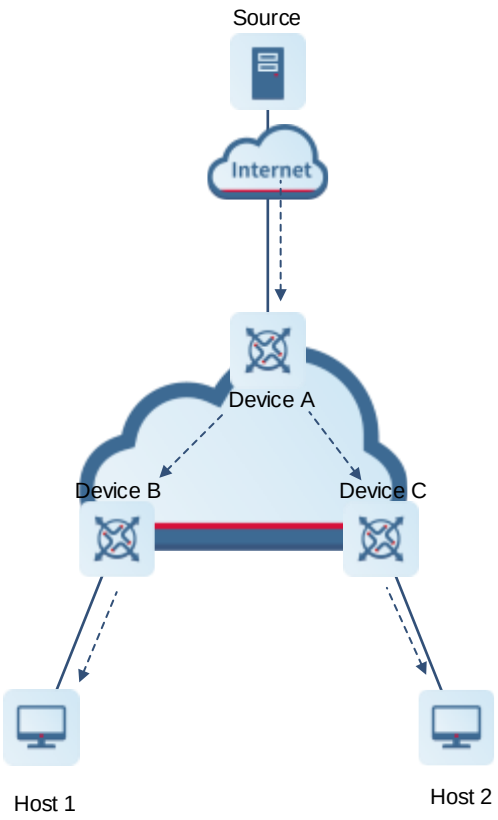
Compared with unicast, multicast reduces redundant traffic, relieves transmission loads of servers and intermediate devices, and completes one-to-multiple content transmission with high efficiency. Multicast is applied to different network services that have high requirements for real timeliness, for example, Internet TV, distance education, live broadcast and multimedia conference.

Proper multicast routes must be configured on the intermediate devices so that IPv4 multicast packets can be correctly forwarded. This chapter describes how to create and maintain IPv4 multicast routes and control multicast packet forwarding based on the multicast routes.

1.1.2 Basic Topology of IPv4 Multicast

Figure 1-2 shows a simple multicast topology that includes a multicast source, multicast devices (Device A, Device B, and Device C), and members in a multicast group.

Figure 1-2 Basic Topology of IPv4 Multicast



As shown in Figure 1-2, the transmission process of a multicast packet is as follows.

(1) The multicast source functions as a packet sender and sends a multicast packet to one or more multicast groups.

(2) The multicast packet is forwarded by the intermediate devices to the packet receivers (members in the multicast group). The intermediate devices are routers or switches that support the multicast function and can correctly forward the multicast packet. They are referred to as multicast devices collectively.

(3) This multicast group contains multiple members and they reside in different network segments on the network. Therefore, the multicast packet sent from the multicast source may be replicated into multiple copies by the multicast devices and then sent to the members in the multicast group.

(4) The members in the multicast group receive the multicast packet from the source.

1.1.3 Basic Concepts of IPv4 Multicast

1. PIM

Protocol Independent Multicast (PIM) is a multicast routing protocol that provides multicast routes based on unicast static routes or unicast routing tables that are generated based on the unicast route protocols. PIM is independent from the unicast routing protocols used and can use the static routes or unicast routing tables that are generated based on any unicast routing protocol, for example, Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Border Gateway Protocol (BGP).

PIM generates multicast routing entries based on the reverse path forwarding (RPF) mechanism, and controls multicast packet forwarding based on the entries. For more information about RPF, see 1.1.5 RPF Checking.

2. Multicast Routing Entry and Forwarding Entry

A multicast routing entry is generated based on multicast routing protocols. Specific routing entries vary with the routing protocols, and they are a comprehension of the routing protocol entries.

A multicast forwarding entry is used to guide multicast packet forwarding, and it is generated based on routing entry information.

3. Multicast Network

Numerous multicast devices constitute a multicast network, and multicast packets are transmitted between multicast sources and members in multicast groups on the network. Multicast packet query and forwarding between multicast devices are completed by running PIM. These PIM running devices are referred to as PIM routers.

PIM takes effect to device interfaces. An interface with PIM enabled is referred to as a PIM interface. A PIM interface that receives a multicast packet is an upstream interface and the interface resides in an upstream network segment. A PIM interface that sends a multicast packet is a downstream interface and the interface resides in a downstream network segment.

PIM routers are connected through PIM interfaces, which constitutes a PIM network.

4. Multicast Border

Data in a multicast network is not transmitted boundlessly. You can configure an access control list (ACL) on a PIM interface of a device to filter multicast packets and allow packets of specific multicast groups to pass. That is, set a border to control multicast packet transmission.

By configuring borders on PIM interfaces, you can divide a large PIM network into multiple PIM domains.

1.1.4 Principle of IPv4 Multicast Forwarding

To ensure correct forwarding of multicast packets by multicast devices, enable multicast routing protocols on the devices.

Upon receiving a multicast packet, a multicast device checks whether the multicast packet is valid and selects proper paths based on the forwarding table to forward the packet to one or more downstream devices. The basic process of IPv4 multicast forwarding is as follows:

(1) A multicast device receives a multicast packet from an upstream interface.

(2) The multicast device queries the multicast forwarding table to obtain proper forwarding paths. If no proper forwarding path is found, the multicast device performs RPF checking to determine forwarding paths and updates the multicast forwarding table.

(3) The multicast device forwards this packet to the outbound interfaces of all the determined forwarding paths.

1.1.5 RPF Checking

1. Basic Principles

In unicast transmission, the destination address in a packet corresponds to a specific address in a network. Provided that the destination address is determined, a network device can determine the outbound interface of the packet. In multicast transmission, a multicast address corresponds to members in a multicast group and a

multicast device does not know the IP address of each member. Therefore, the receiver addresses cannot be determined based on the destination address.

RPF checking is used to determine outbound interfaces of a multicast packet. The core idea behind RPF checking is that: An RPF route is generated to check whether the theoretical destination interface of a multicast packet is consistent with the actual interface. If they are not consistent, the packet is discarded. If they are consistent, the packet is forwarded to all the determined outbound interfaces.

2. RPF Checking Procedure

The RPF checking procedure consists of the following steps:

(1) Select optimal routes.

Take the address (the source IP address in a multicast packet) of the multicast source as the destination address and select optimal routes from the local device to the destination address.

The optimal routes are selected from the unicast routing table, Multiprotocol Extensions for BGP-4 (MBGP) routing table, and multicast static routing table, respectively.

(2) Determine an RPF route.

Select a route from the determined optimal routes of the routing tables as an RPF route based on rules. Table 1-1 lists the specific rules.

Table 1-1 RPF Routing Rules

Select RPF Route Based on the Longest Match	Rule Priority (a Smaller Number Indicates a Higher Priority)	Description
No	1	The route with the highest priority is selected.
	2	An RPF route is selected in the sequence of multicast static route, MBGP route, and unicast route.
Yes	1	The route with the longest match mask is selected.
	2	The route with the highest priority is selected.
	3	An RPF route is selected in the sequence of multicast static route, MBGP route, and unicast route.

An RPF route includes RPF interface information and the information is used for checking the RPF interface.

- In a unicast route and an MBGP route, the outbound interface in a routing entry is used as an RPF interface, with the next hop being an RPF neighbor.
- In a multicast static routing entry, the RPF interface and RPF neighbor are specified.

(3) Check the RPF interface.

Check whether the inbound interface of the multicast packet is consistent with the RPF interface.

- If yes, the RPF interface passes the checking.
- Otherwise, the RPF interface fails the checking.

1.1.6 RPF Checking and Multicast Packet Forwarding

When a multicast packet is forwarded, query a path from the forwarding table first. If no proper path is found, RPF checking is performed. Path information that is generated after RPF checking passes is updated to the forwarding table and can be queried for packet forwarding next time.

The rules of forwarding a multicast packet are as follows:

- No forwarding entry exists in a multicast forwarding table.

  RPF checking is performed for this packet. The RPF interface is used as an inbound interface and updated to the forwarding table.

  - If the RPF interface passes the checking, the packet is forwarded to all outbound interfaces.
  - If the RPF interface fails the checking, this packet is discarded.
- There are forwarding entries in a multicast forwarding table.
  - If the inbound interface of the packet matches the inbound interface in an entry, the packet is forwarded to all outbound interfaces.
  - If the inbound interface of the packet does not match the inbound interface in an entry, RPF checking is performed. If the RPF interface is consistent with the inbound interface in an entry, the packet is discarded. If the RPF interface is not consistent with the inbound interface in an entry, the inbound interface in the entry is updated as an RPF interface and the inbound interface in the packet is compared with the RPF interface to determine whether they are consistent.

1.2 Restrictions and Guidelines

- All the configuration items must be configured after the basic functions of IPv4 multicast are configured.
- The multicast routing function is implemented based on unicast routes. Before applying the multicast function, ensure that the unicast communication between network nodes is normal.

1.3 Configuration Task Summary

IPv4 multicast route management configuration includes the following tasks:

(1) Configuring Basic Functions of IPv4 Multicast

(2) (Optional) Configuring a packet forwarding rule. The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configuring RPF Route Selection Based on the Longest Match Rule
- Configuring Static Routes of IPv4 Multicast
- Configuring IPv4 Multicast Borders
- Configuring L2 Direction Control for Multicast Streams
- Configuring TTL Threshold
- Configuring Forced Forwarding of Multicast Packets by Software

(3) (Optional) Configuring multicast entries. The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configuring Entry Capacity of IPv4 Multicast Routing Table

- Configuring the Overwriting Mechanism upon Overflow of Multicast Hardware Forwarding Entries

(4) (Optional) Configuring Multicast Non-Stop Forwarding Parameters

1.4 Configuring Basic Functions of IPv4 Multicast

1.4.1 Overview

To configure basic functions of IPv4 multicast, enable the IPv4 multicast routing function and the IPv4 multicast protocols on a device so that the device has the multicast packet forwarding function and can provide IPv4 multicast services for multicast sources and hosts in multicast groups.

1.4.2 Restrictions and Guidelines

- The IPv4 multicast routing function should be enabled on each router unless otherwise specified.
- IPv4 unicast routes must be configured so that PIM can use the unicast routes to generate multicast routes.
- After L3 multicast is enabled for a private virtual local area network (PVLAN) and a super VLAN, if there is a multicast source in a sub VLAN, the entry count increases by 1. This is because the inbound validity will be checked during multicast forwarding, and therefore an extra entry will be generated, and the inbound of this entry is the sub VLAN that the multicast stream enters.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IPv4 multicast routing.

ip multicast-routing

The multicast routing function is disabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Enable an IPv4 multicast protocol on an interface. Select at least one of them to configure.

- Enable Protocol Independent Multicast Dense Mode (PIM-DM) on the interface.

  ip pim dense-mode

  PIM-DM is disabled for an interface by default.

  PIM-DM is a multicast routing protocol that is used in dense mode and applies to small-sized networks where members in a multicast group are densely distributed. For more information about PIM-DM, see *Configuring PIM-DM*.

- Enable Protocol Independent Multicast Sparse Mode (PIM-SM) on the interface.

  ip pim sparse-mode

  PIM-SM is disabled for an interface by default.

PIM-SM is a multicast routing protocol that is used in sparse mode and applies to large-sized networks where members in a multicast group are sparsely distributed. For more information about PIM-SM, see *Configuring PIM-SM*.

1.5 Configuring RPF Route Selection Based on the Longest Match Rule

1.5.1 Overview

In multicast routing, there may be different routing tables, for example, multicast static routing table, MBGP routing table, and unicast routing table. An optimal route should be selected from all the routing tables and used as an RPF route.

If the longest match rule is used, the route with the longest match mask is selected from the optimal routes in different routing tables as the RPF route. If the masks are equal in length, the route with the highest priority is selected from the optimal routes. If the priorities are consistent, a route is selected in the sequence of multicast static route, MBGP route, and unicast route.

1.5.2 Restrictions and Guidelines

The longest match rule can be configured on each device unless otherwise specified.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure RPF route selection based on the longest match rule.

ip multicast rpf longest-match

By default, the route with the highest priority is selected as the RPF route. If they have the same priority, the RPF routes are selected in the sequence of multicast static route, MBGP route, and unicast route.

1.6 Configuring Static Routes of IPv4 Multicast

1.6.1 Overview

You can configure static routes of IPv4 multicast to specify RPF interfaces or RPF neighbors for multicast packets from specific multicast sources. This function can be used to change and connect RPF routes.

- Change an RPF route: If you want a device to receive multicast packets from a multicast source through a specified interface, but this interface is not the required interface based on the RPF checking result, you need to configure a multicast static route to specify this required interface as an RPF interface.
- Connect an RPF route: If a unicast route is interrupted, a multicast route failed to be generated by RPF. You can configure a multicast static route to specify an RPF interface to complete RPF checking and realize multicast packet forwarding.

1.6.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a multicast static route.

ip mroute *source-address mask* { [**bgp** | **isis** | **ospf** | **rip** | **static**] { *rpf-addrress* | *interface-type interface-number* } } [*distance*]

No multicast static route is configured by default. To specify an outbound interface for a multicast static route, set the outbound interface to point-to-point type.

1.7 Configuring IPv4 Multicast Borders

1.7.1 Overview

After IPv4 multicast borders are configured, a multicast network can be divided into different domains so that specified multicast packets are transmitted in a domain.

The multicast border function filters out specified multicast packets based on an ACL to forbid packets of this type from entering or leaving an interface.

1.7.2 Restrictions and Guidelines

IP multicast borders can be configured on each PIM router interface unless otherwise specified.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an IP multicast border.

ip multicast boundary *access-list* [**in** | **out**]

No multicast border is configured by default.

This command can associate a standard ACL with an extended ACL. For an extended ACL, only the destination address is matched and the source address is not matched.

1.8 Configuring L2 Direction Control for Multicast Streams

1.8.1 Overview

By configuring L2 direction control for multicast streams, you can control multicast stream forwarding on an interface.

You can configure this command multiple times for a multicast stream. That is, configure multiple interfaces to forward the stream. After direction control is configured for a multicast stream, this multicast stream can be forwarded only by these configured interfaces. Other interfaces are not allowed to forward the stream.

1.8.2 Restrictions and Guidelines

This command controls only the forwarding of multicast streams on interfaces, but does not directly affect the processing of protocol packets by the multicast protocols. However, some features of the multicast protocols (PIM-DM or PIM-SM) depend on the multicast streams. Behaviors of the multicast routing protocols may be affected.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure L2 direction control for multicast streams.

ip multicast static *source-address group-address interface-type interface-number*

No L2 direction control is configured for multicast streams by default.

1.9 Configuring TTL Threshold

1.9.1 Overview

The time to live (TTL) value in an IP packet is used to define the maximum number of hops that this packet can transmit through.

To configure a TTL threshold means to configure the minimum TTL value of multicast packets allowed on an interface. Before forwarding a multicast packet on an interface, the device checks whether the TTL value in the packet is greater than the TTL threshold. If yes, the device forwards the packet. Otherwise, the device discards this packet.

1.9.2 Restrictions and Guidelines

- A TTL threshold can be configured on each PIM router interface unless otherwise specified.
- The TTL threshold must be configured on router interfaces and takes effect only to multicast packets.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a TTL threshold for an interface.

ip multicast ttl-threshold *ttl-threshold-value*

The default TTL threshold for an interface is **0**.

1.10 Configuring Forced Forwarding of Multicast Packets by Software

1.10.1 Overview

After the mechanism of forced forwarding of multicast packets by software is configured, multicast packets destined to the local device can be forwarded to other interfaces by software.

1.10.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable forced forwarding of multicast packets by software.

msf force-forwarding

The mechanism of forced forwarding of multicast packets by software is disabled by default.

1.11 Configuring Entry Capacity of IPv4 Multicast Routing Table

1.11.1 Overview

A device creates and maintains a multicast route forwarding entry for each received multicast packet. Therefore, the entry quantity increases continuously. If the number of entries maintained by a device surpasses the limited hardware resources of the device, hardware forwarding may be changed to software forwarding, which consumes device memory and reduces device performance.

The entry capacity of an IPv4 multicast routing table refers to the maximum number of entries that can be added to the IPv4 multicast routing table. The entry capacity of an IPv4 multicast routing table is 1000 entries by default, and it can be configured based on actual network situation and service performance without affecting running of the device.

1.11.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure entry capacity of an IPv4 multicast routing table.

ip multicast route-limit *route-limit* [*max-threshold*]

The default entry capacity of an IPv4 multicast routing table is **1000** entries.

1.12 Configuring the Overwriting Mechanism upon Overflow of Multicast Hardware Forwarding Entries

1.12.1 Overview

The hardware forwarding entries are limited. If they are used up, the device uses software forwarding entries. Compared with hardware forwarding entries, software forwarding entries feature lower performance, occupy device memory, and deteriorate device performance.

After the overwriting mechanism upon overflow of multicast hardware forwarding entries is enabled, new entries can overwrite the earliest entries when hardware forwarding entries are used up.

1.12.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the overwriting mechanism upon overflow of multicast hardware forwarding entries.

msf ipmc-overflow override

The overwriting mechanism upon overflow of multicast hardware forwarding entries is disabled by default.

1.13 Configuring Multicast Non-Stop Forwarding Parameters

1.13.1 Overview

On a device that includes multiple management boards, after a management board is switched over, multicast protocols such as PIM-SM and Internet Group Management Protocol (IGMP) Snooping need re-convergence. You can configure non-stop forwarding parameters to ensure continuous forwarding of multicast streams during re-convergence of the multicast protocols.

1.13.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure multicast non-stop forwarding parameters.

msf nsf { **convergence-time** *convergence-time* | **leak** *leak-time* }

The maximum period for multicast protocol convergence is **20** seconds and the packet leakage time is **30** seconds by default.

After the configured protocol convergence period times out, all multicast forwarding entries that are not updated during the convergence period are deleted.

1.14 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information of the **debug** command occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

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

Table 1-2 Monitoring

Command	Purpose
clear ip mroute { * | *group-address* [*source-address*] }	Clears the IPv4 multicast forwarding table.
clear ip mroute statistics { ***** | *group-address* [*source-address*] }	Resets the statistics in the IPv4 multicast forwarding table.
show ip mroute summary	Displays the IPv4 multicast forwarding table.
show ip mroute static	Displays the information about IPv4 multicast static route.
show ip rpf *source-address*	Displays the RPF information of a specified IPv4 source address.
show ip mvif [*interface-type interface-number*]	Displays the information about IPv4 multicast interfaces.
show ip mrf mfc	Displays the IPv4 L3 multicast forwarding table.
show msf nsf	Displays the configuration of IPv4 multicast non-stop forwarding.
show msf msc	Displays the IPv4 multi-layer multicast forwarding table.
debug nsm mcast all	Debugs the running procedure of the multicast core.
debug nsm mcast fib-msg	Debugs the communication procedure between the IPv4 multicast core and the protocol module.

Command	Purpose
debug nsm mcast vif	Debugs the interface running procedure about the IPv4 multicast core.
debug nsm mcast stats	Debugs the interface and entry statistics processing procedure about the IPv4 multicast core.
debug ip mrf forwarding	Debugs the IPv4 L3 multicast packet forwarding procedure.
debug ip mrf mfc	Debugs the operation procedure of L3 multicast forwarding entries on an IPv4 network.
debug ip mrf event	Debugs the processing procedure of L3 multicast forwarding events on an IPv4 network.
debug msf forwarding	Debugs the IPv4 multi-layer multicast packet forwarding procedure.
debug msf msc	Debugs the operation procedure of multi-layer multicast forwarding entries on an IPv4 network.
debug msf ssp	Debugs the bottom-layer hardware processing procedure of IPv4 multi-layer multicast forwarding.
debug msf api	Debugs the API calling procedure of IPv4 multi-layer multicast forwarding.
debug msf event	Debugs the processing procedure of multi-layer multicast forwarding events on an IPv4 network.

-

1.15 Common Misconfigurations

- An IPv4 unicast route is incorrectly configured.
- IPv4 multicast routing is not enabled on a router.

Contents

1 Configuring IGMP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Basic Principles of IGMPv1 1
1.1.3 Basic Principles of IGMPv2 3
1.1.4 Basic Principles of IGMPv3 4
1.1.5 IGMP SSM Mapping 5
1.1.6 IGMP Proxy 5
1.1.7 Protocols and Standards 6
1.2 Configuration Task Summary 6
1.3 Configuring Basic Functions of IGMP 6
1.3.1 Overview 6
1.3.2 Restrictions and Guidelines 7
1.3.3 Procedure 7
1.4 Configuring IGMP Parameters 7
1.4.1 Configuration Tasks 7
1.4.2 Configuring an IGMP Version 7
1.4.3 Configuring the Maximum Response Time for Query Packets 8
1.4.4 Configuring Common Group Query 8
1.4.5 Configuring Specific Group Query 9
1.4.6 Configuring Survival Period of Other Querier 9
1.5 Configuring IGMP Group Filtering 10

1.5.1 Configuration Tasks 10

1.5.2 Filtering a Multicast Group 10

1.5.3 Configuring the Maximum Number of Group Members 11

1.6 Configuring the IGMP Proxy Function 12

1.6.1 Overview 12

1.6.2 Restrictions and Guidelines 12

1.6.3 Procedure 12

1.7 Configuring the IGMP SSM Mapping Function 13

1.7.1 Overview 13

1.7.2 Restrictions and Guidelines 13

1.7.3 Procedure 13

1.8 Configuring the Router Alert Option of IGMP Packets 13

1.8.1 Overview 13

1.8.2 Restrictions and Guidelines 14

1.8.3 Procedure 14

1.9 Enabling Source Address Checking for IGMP Report Packets 14

1.9.1 Overview 14

1.9.2 Procedure 14

1.10 Enabling Fast Leave 15

1.10.1 Overview 15

1.10.2 Restrictions and Guidelines 15

1.10.3 Procedure 15

1.11 Configuring the Querier Robustness Variable 15

1.11.1 Overview 15

1.11.2 Procedure 15

1.12 Adding a Static Interface to a Group 16

1.12.1 Procedure 16

1.13 Simulating a Host to Join a Group 16

1.13.1 Overview 16

1.13.2 Procedure 16

1.14 Monitoring 16

1 Configuring IGMP

1.1 Introduction

1.1.1 Overview

Multicast devices in a multicast network must maintain members in a multicast group that are connected to the same network segment with the multicast devices. Hosts need to be added to the multicast group dynamically so that a multicast packet can be correctly transmitted to the hosts that need the packet. With the development of multicast applications and ever growing of the multicast network, a protocol is needed to manage the members in the multicast group.

The Internet Group Management Protocol (IGMP) is a TCP/IP protocol that manages members in an IPv4 multicast group and runs on the multicast devices and hosts residing on the stub of the multicast network, creating and maintaining membership of the multicast group between the hosts and connected multicast devices. At present, IGMP is available in three versions: IGMPv1, IGMPv2, and IGMPv3. The three versions support the Any-Source Multicast (ASM) and Source-Specific Multicast (SSM) models as follows:

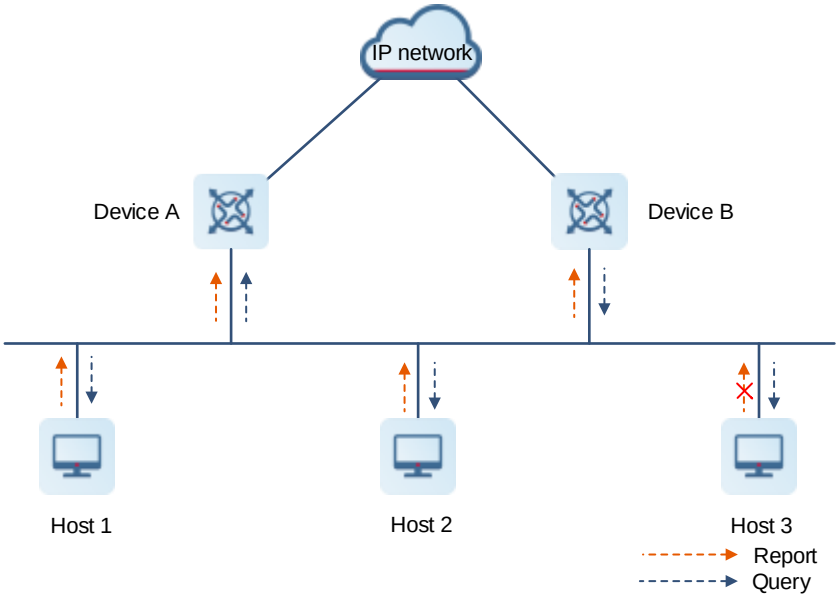
- The three versions of IGMP support the ASM model.
- IGMPv3 can be directly applied to the SSM model.
- IGMPv1 and IGMPv2 can be applied to the SSM model only when the IGMP SSM mapping technology is configured.

1.1.2 Basic Principles of IGMPv1

IGMPv1 runs on multicast devices and hosts, and manages members in a multicast group by communication between the multicast devices and hosts. The IGMP behavior of a multicast device is referred to as device behavior, and the IGMP behavior of a host is referred to as host behavior.

1. Basic Structure of IGMPv1

Figure 1-1 Basic Topology of IGMP



As shown in Figure 1-1, IGMP runs on hosts (host 1, host 2, and host 3) that need to be added to a multicast group and multicast devices (device A and device B) that are directly connected to the hosts.

A host sends an IGMP Report packet to a multicast device to report that the host joins the multicast group. The multicast device sends an IGMP Query packet to the host to discover the membership of the multicast group.

There are two important concepts involved in IGMPv1 running:

- Querier

  A querier is a multicast device that sends query packets and receives packets of a host. The querier is used to discover members of a multicast group on a connected network segment.

  If multiple multicast devices running IGMP reside on a network segment, one of the multicast devices is selected as a querier, and other devices function as non-queriers. In IGMPv1, a designated router (DR) elected based on the multicast routing protocols functions as a querier. For more information about DR, see *Configuring PIM-SM*.

- IGMPv1 packet

  IGMPv1 packets are classified into IGMP Query packets and IGMP Report packets.

  - IGMP Query packet: A packet sent by a multicast device to a host to query members of a multicast group on the connected network segment.
  - IGMP Report packet: A packet sent by a host to a multicast device to join a multicast group.

2. Work Process of IGMPv1

Management of multicast group members is divided into host joining a multicast group and host leaving from the multicast group.

- Host joining a multicast group

  Communication after a host joins a multicast group falls into active joining and response query.

- Active joining steps are as follows:

  When a host initiates a join request, the host sends an IGMP Report packet to the network segment it resides, to report that it joins a multicast group.

  The querier receives the IGMP Report packet, and creates a forwarding entry for the members in the multicast group.

- Response query steps are as follows:

  The querier periodically sends an IGMP Query packet to all hosts in the local network segment in multicast mode.

  The host that joins the multicast group replies an IGMP Report packet to the querier in multicast mode. Other hosts that do not join the multicast group do not respond.

  The querier creates and maintains forwarding entries for the members in each multicast group.

- Host leaving a multicast group

  a A host leaves a multicast group without notifying the querier (types of packets for leaving a multicast group are not defined in IGMPv1).

  a The querier does not receive an IGMP Report packet from a multicast group in a specified period and removes the forwarding entry of this multicast group after the specified timer times out.

1.1.3 Basic Principles of IGMPv2

On the basis of the features of IGMPv1, IGMPv2 comes with a querier election mechanism and a group leaving mechanism.

1. Querier Election Mechanism

In IGMPv1, no querier election rule exists, a DR is selected as a querier using multicast routing protocols. In IGMPv2, a querier election mechanism is developed. The main communication process is as follows:

(1) A multicast device running IGMPv2 considers itself a querier and sends an IGMP Query (common group) packet (with destination address 224.0.0.1) to the connected network segment.

(2) Upon receiving the query packet, another multicast device compares the source IP address in the packet with the local IP address. If the source IP address is smaller than the local IP address, the querier changes to a non-querier. In this way, only one querier survives finally on the connected network segment.

(3) After the multicast device changes to a non-querier, a timer starts. The timeout time of the timer is referred to as "survival period of other querier". After timer times out, the multicast device considers itself a querier and re-initiates a querier election process. If the multicast device receives an IGMP Query packet from the querier before the timer times out, the timer is reset.

2. Group Leaving Mechanism

In IGMPv1, a host leaves a multicast group without notifying the multicast device. The multicast device detects the leaving of the host in hindsight only after the timer times out. In IGMPv2, an IGMP Leave packet is developed. When a host leaves the multicast group, the host sends an IGMP Leave packet to notify the multicast device. The main communication process is as follows:

(1) When a host leaves a multicast group, the host sends an IGMP Leave packet to all multicast devices (destination address 224.0.0.2) on the connected network segment.

(2) Upon receiving the packet, the querier sends a query packet (the destination address is the multicast group address that the host resides) of the specified multicast group to the connected network segment.

(3) If this multicast group contains other hosts, the hosts reply an IGMP Report packet to the querier within the maximum response time upon receiving the query packet.

(4) If the querier receives replies from the hosts of the multicast group within the maximum response time, there are members in the multicast group. The querier continues maintaining the forwarding entry of this multicast group. Otherwise, the querier clears the entry of this multicast group.

1.1.4 Basic Principles of IGMPv3

On the basis of the features of IGMPv1 and IGMPv2, IGMPv3 comes with a multicast source filtering function and enhanced IGMP Query packet and IGMP Report packet.

1. Multicast Source Filtering Function

The multicast source filtering function requires the cooperation of the querier and a host.

- Host action

  A host supports filtering of a specific multicast source. When the host tries to join a multicast group, it adds information of one or multiple sources to an IGMP Report packet and sets the mode of the multicast sources to INCLUDE or EXCLUDE. In INCLUDE mode, the host receives packets from this multicast source. In EXCLUDE mode, the host rejects packets from this multicast source.

- Querier action

  When receiving multicast source information in INCLUDE mode, the multicast device acts as follows:

  - If this multicast source is active, the multicast device forwards the packet from this multicast source.
  - If this multicast source is inactive, the multicast device does not forward the packet from this multicast source.

  When receiving multicast source information in EXCLUDE mode, the multicast device acts as follows:

  - If other hosts need packets from this multicast source, the multicast device continues forwarding the packet from this multicast source.
  - If this multicast source is inactive, the multicast device does not forward the packet from this multicast source.
  - For other multicast sources not in EXCLUDE mode, the multicast device needs to forward the packets.

2. Enhanced IGMP Query Packet and IGMP Report Packet

- Enhanced IGMP Query Packet

  IGMPv1 supports common group query, and IGMPv2 supports specific group query. On the basis of the features of IGMPv1 and IGMPv2, IGMPv3 supports specific source and group query.

  - Common group query: No multicast source or group is specified.
  - Specific group query: A multicast group is specified.
  - Specific source and group query: A multicast source and a multicast group are specified.

- Enhanced IGMP Report Packet

  In IGMPv3, an IGMP Report packet carries records of one or multiple groups. The group records include the multicast source addresses and multicast group addresses.

Group records are divided into the following types:

- IS_IN: The filtering mode of a multicast source is INCLUDE, indicating that only packets from this specified multicast source to this multicast group are received.
- IS_EX: The filtering mode of a multicast source is EXCLUDE, indicating that packets from this specified multicast source to this multicast group are rejected.
- TO_IN: The filtering mode is changed from EXCLUDE to INCLUDE.
- TO_EX: The filtering mode is changed from INCLUDE to EXCLUDE.
- ALLOW: Multicast packets from specified multicast sources to this multicast group are received. If the filtering mode is INCLUDE, these multicast sources are added to the original source list. If the filtering mode is EXCLUDE, these multicast sources are removed from the original source list.
- BLOCK: Multicast packets from specified multicast sources to this multicast group are rejected. If the filtering mode is INCLUDE, these multicast sources are removed from the original source list. If the filtering mode is EXCLUDE, these multicast sources are added to the original source list.

1.1.5 IGMP SSM Mapping

In actual network environment, most multicast devices support IGMPv3. However, there are a great number of old multicast devices that support only IGMPv1 or IGMPv2. Consequently, these old multicast devices cannot provide hosts with the multicast services in the SSM model using IGMPv3. After the IGMP SSM mapping technology is applied, the multicast devices can provide hosts with the multicast services in the SSM model without upgrading to IGMPv3.

The IGMP SSM mapping technology enables the multicast devices to support IGMPv3 by mapping the multicast group information in IGMPv1 Report packets and IGMPv2 Report packets to the multicast group information that carries specific multicast sources. After an SSM mapping rule is configured on the multicast devices, upon receiving IGMPv1 Report packets and IGMPv2 Report packets, the multicast devices process the packets based on the multicast group information in the packets.

- If a multicast group is not in the SSM group address range, the multicast services are provided in the ASM model.
- If the multicast group is in the SSM group address range and no SSM mapping rule corresponding to this multicast group is configured on the multicast device, the multicast device cannot provide multicast services in the SSM model and then discards the packets.
- If the multicast group is in the SSM group address range and an SSM mapping rule corresponding to this multicast group is configured on the multicast device, the multicast group information in the packets is converted to the multicast group information that carries specific multicast sources and the multicast device provides the multicast services in the SSM model.

1.1.6 IGMP Proxy

In a simple tree network topology, a border multicast device does not need to run complex multicast routing protocols such as Protocol Independent Multicast (PIM), you can configure the IGMP proxy function on this multicast device. This multicast device functions as an intermediate proxy between upstream IGMP querier and downstream hosts.

A device running the IGMP proxy functions as a multicast device and a host at the same time. For an upstream IGMP querier, this device plays the role of a host and executes host actions. For a downstream host, this device plays the role of an IGMP querier and executes querier actions.

1.1.7 Protocols and Standards

- RFC 1112: Host Extensions for IP Multicasting
- RFC 2236: Internet Group Management Protocol, Version 2
- RFC 3376: Internet Group Management Protocol, Version 3
- RFC 4605: Internet Group Management Protocol (IGMP)/Multicast Listener Discovery

1.2 Configuration Task Summary

IGMP configuration includes the following tasks:

- Configuring Basic Functions of IGMP
- (Optional) Configuring IGMP Parameters. All the configuration tasks below are optional. Select the configuration tasks as required.
  - Configuring an IGMP Version
  - Configuring the Maximum Response Time for Query Packets
  - Configuring Common Group Query
  - Configuring Specific Group Query
  - Configuring Survival Period of Other Querier
- (Optional) Configuring IGMP Group Filtering
- (Optional) Configuring the IGMP Proxy Function
- (Optional) Configuring the IGMP SSM Mapping Function
- (Optional) Configuring the Router Alert Option of IGMP Packets
- (Optional) Enabling Source Address Checking for IGMP Report Packets
- (Optional) Enabling Fast Leave
- (Optional) Configuring the Querier Robustness Variable
- (Optional) Adding a Static Interface to a Group
- (Optional) Simulating a Host to Join a Group

1.3 Configuring Basic Functions of IGMP

1.3.1 Overview

Basic functions of IGMP lay a foundation for other functions, enable multicast devices to run IGMP, and help collect and manage members in a multicast group.

You cannot directly enable the basic functions of IGMP. You need to enable the multicast routing function on a device to make the basic functions of IGMP take effect.

1.3.2 Restrictions and Guidelines

Before the basic functions of IGMP are enabled, you must enable the Protocol Independent Multicast Sparse Mode (PIM-SM) or Protocol Independent Multicast Dense Mode (PIM-DM) function on an interface to make the basic functions of IGMP take effect. To disable the basic functions of IGMP take effect, you need to remove the configuration of the PIM-SM or PIM-DM function.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IPv4 multicast routing.

ip multicast-routing

The multicast routing is disabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Enable the PIM-SM or PIM-DM function on an interface. Select at least one of them to configure.

- Enable PIM-DM on an interface.

  ip pim dense-mode

  The PIM-DM function is disabled on an interface by default.

- Enable PIM-SM on an interface.

  ip pim sparse-mode

  The PIM-SM function is disabled on an interface by default.

1.4 Configuring IGMP Parameters

1.4.1 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring an IGMP Version
- Configuring the Maximum Response Time for Query Packets
- Configuring Common Group Query
- Configuring Specific Group Query
- Configuring Survival Period of Other Querier

1.4.2 Configuring an IGMP Version

1. Overview

IGMP comes with three versions: IGMPv1, IGMPv2, and IGMPv3. A later version corresponds to stronger protocol functions. You can select an IGMP version based on network requirements and IGMP support of upstream and downstream devices.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an IGMP version.

ip igmp version { **1** | **2** | **3** }

IGMPv2 runs on an interface by default.

After this command is run, the IGMP function module automatically restarts.

1.4.3 Configuring the Maximum Response Time for Query Packets

1. Overview

After sending a query packet, the querier needs to receive a reply packet from a host in the specified time. Otherwise, the querier considers that no member exists in the corresponding multicast group and deletes the group information. This specified time is referred to as the maximum response time for a query packet, and it can be set to a proper time value based on actual network topology.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum response time for query packets on an interface.

ip igmp query-max-response-time *query-max-response*

The maximum response time for query packets on an interface is **10** seconds by default.

1.4.4 Configuring Common Group Query

1. Overview

Common group query means querying members in a multicast group. You can configure an interval for sending common group query packets.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the interval for querying a common group member.

ip igmp query-interval *query-interval*

The interval for querying a common group member is **125** seconds by default.

1.4.5 Configuring Specific Group Query

1. Overview

Specific group query means querying members in a specified multicast group. You can configure an interval and times for sending specific group query packets.

Upon receiving an IGMP Leave packet on an interface, the querier continuously sends specific group query packets and waits for responses from hosts. If no host replies in the specified time, the querier considers that this multicast group does not contain any member, and deletes this interface from the IGMP group member records. Then, this interface does not forward packets from this multicast group. The timeout time is a product of the number of specific group query packets and the times for sending the specific group query packets.

2. Restrictions and Guidelines

The parameter of specific group query can be configured in IGMPv2 and IGMPv3. The parameter is not supported in IGMPv1.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the parameters of specific group query. Select at least one of them to configure.

- Configure the interval for sending specific group query packets.

  ip igmp last-member-query-interval *last-member-query-interval*

  The interval for sending specific group query packets is **1** second by default.

- Configure the times for sending specific group query packets.

  ip igmp last-member-query-count *last-member-query-count-number*

  Specific group query packets are sent twice by default.

1.4.6 Configuring Survival Period of Other Querier

1. Overview

A querier election mechanism is introduced in IGMPv2. Based on the mechanism, non-queriers maintain a timer and the timeout time of the timer is referred to as "survival period of other querier". If the timer times out, a multicast device considers itself a querier and re-initiates a querier election request. During networking, you can determine proper survival period of other querier based on network topology configuration.

2. Restrictions and Guidelines

The querier election mechanism can be configured in IGMPv2 and IGMPv3. It is not supported in IGMPv1.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure survival period of other querier.

ip igmp query-timeout *query-timeout*

The survival period of other querier is **255** seconds by default.

1.5 Configuring IGMP Group Filtering

1.5.1 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Filtering a Multicast Group
- Configuring the Maximum Number of Group Members

1.5.2 Filtering a Multicast Group

1. Overview

If you do not want hosts in the network segment where an interface resides to join a multicast group, you can configure access control list (ACL) rules on the interface as a filter. The interface filters IGMP Report packets of the hosts based on the ACL rules and allows the hosts to join specific groups.

2. Restrictions and Guidelines

- For more information about ACL, see *Configuring ACL*.
- Extended ACL rules can be configured in IGMPv3. When a received IGMP Report packet is (S1, S2, S3…Sn, G), an ACL rule is used to match (0, G). Therefore, to normally filter (S1, S2, S3…Sn, G), a (0, G) extended ACL rule must be configured.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Filter out groups that you do not want a host to join.

ip igmp access-group { *acl-name* | *acl-number* }

Hosts can join any group by default.

1.5.3 Configuring the Maximum Number of Group Members

1. Overview

To configure the maximum number of group members means configuring the maximum number of multicast groups that a host can join.

The configuration can be completed in interface or global mode. If the configuration is completed in global mode, the number of group members for a multicast device is limited. If the configuration is completed in interface mode, the number of group members on an interface is limited. If the number of group member records exceeds the interface limit or global limit, subsequent received IGMP Report packets are ignored.

2. Restrictions and Guidelines

- Group member records that are generated in EXCLUDE mode list are not counted in the group members.
- Interface and global limits can be configured separately. If the global limit is smaller than the interface limit, the global limit prevails.

3. Procedure (Global Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of IGMP group members in global configuration mode.

ip igmp limit *limit-number* [**except** *acl-name* | **except** *acl-number*]

The maximum number of IGMP group members is **64000** in global configuration mode by default.

4. Procedure (Interface Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum number of IGMP group members on an interface.

ip igmp limit *limit-number* [**except** *acl-name* | **except** *acl-number*]

The maximum number of IGMP group members on an interface is **4000** by default.

1.6 Configuring the IGMP Proxy Function

1.6.1 Overview

In a simple tree network topology, you can configure the IGMP proxy function and use it as an intermediate proxy between upstream IGMP querier and downstream hosts without running complex multicast routing protocols such as PIM.

On the device that runs the IGMP proxy, interfaces are classified into proxy service interfaces and MRoute proxy interfaces.

The proxy service interfaces execute host behaviors, receive IGMP packets from upstream devices, and forward the packets to the MRoute proxy interfaces.

The MRoute proxy interfaces execute device behaviors, receive IGMP Report packets from downstream devices, and forward the packets to the proxy service interfaces.

1.6.2 Restrictions and Guidelines

- The basic functions of IGMP must be configured.
- The interfaces connected to upstream devices must be configured as proxy service interfaces and the interfaces connected to hosts must be configured as MRoute proxy interfaces. The two types of interfaces must be used at the same time. If only one type of interfaces are configured, the IGMP proxy function will be abnormal.
- If the proxy service interfaces are switched over from L3 to L2, the routing proxy configured on the MRoute proxy interfaces is automatically disabled.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the IGMP proxy function. The configuration steps below are mutually exclusive. Please configure only one task.

- Configure an interface as a proxy service interface.

  ip igmp proxy-service

  No interface is configured as a proxy service interface by default.

  The interface directly connected to an upstream device can be configured as a proxy service interface unless otherwise specified. A device supports 32 proxy service interfaces at most. When a proxy service interface receives an IGMP Report packet, the proxy service interface makes response based on the IGMP group member records.

- Configure an interface as an MRoute proxy interface.

  ip igmp mroute-proxy *interface-type interface-number*

No interface is configured as an MRoute proxy interface by default.

The interface directly connected to a downstream device can be configured as an MRoute proxy interface unless otherwise specified.

1.7 Configuring the IGMP SSM Mapping Function

1.7.1 Overview

At present, the SSM multicast model (supporting filtering multicast sources) is supported in IGMPv3 only. To enable the SSM multicast model to be supported in IGMPv1 and IGMPv2, you can configure the IGMP SSM mapping function on a device, and add multicast group information of specified multicast sources to IGMPv1 and IGMPv2 packets so that the hosts can use the SSM multicast services provided by the device on the basis of running IGMPv1 or IGMPv2.

1.7.2 Restrictions and Guidelines

- When a device receives an IGMPv1 or IGMPv2 Report packet, the device adds the static mapping source address.
- The IGMP SSM mapping function applies to only IGMPv1 and IGMPv2 packets. You are advised to enable IGMPv3 on an interface to ensure that IGMP packets of different versions can obtain the SSM multicast services.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IGMP SSM mapping function.

ip igmp ssm-map enable

The IGMP SSM mapping function is disabled by default.

(4) Configure a static mapping entry.

ip igmp ssm-map static { *acl-name* | *acl-number* } *source-address*

No static mapping entry is configured by default.

1.8 Configuring the Router Alert Option of IGMP Packets

1.8.1 Overview

The Router Alert option in an IP packet header is used to warn a router device to check content in the IP packet. The router device can determine whether to add this option to a packet to be sent and whether to check this option in a received packet. The device does not check this option by default.

After the Router Alert option is configured, if an IGMP packet carries the Router Alert option, the multicast device checks the IGMP packet carefully and updates the controlled content. If the IGMP packet does not carry

the Router Alert option, the multicast device does not check the content in the packet and directly forwards the packet.

1.8.2 Restrictions and Guidelines

After the Router Alert option is configured, the multicast device must add this option to a packet to be sent and check this option in a received packet. Otherwise, an error occurs in IGMP packet receiving.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure to check the Router Alert option in an IGMP packet.

ip igmp enforce-router-alert

The Router Alert option in an IGMP packet is not checked by default.

After this option is configured, IGMP packets that do not carry the Router Alert option are discarded.

(4) Add the Router Alert option to an IGMP packet to be sent.

ip igmp send-router-alert

The Router Alert option is not added to an IGMP packet to be sent by default.

1.9 Enabling Source Address Checking for IGMP Report Packets

1.9.1 Overview

To prevent false packets, you can enable the source address checking function for IGMP packets so that a multicast device receives only IGMP Report packets whose source addresses are on the same network segment as the receiving interface.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable source address checking for IGMP Report packets.

ip igmp enforce-source-subnet

The source address checking function for IGMP Report packets is disabled by default.

1.10 Enabling Fast Leave

1.10.1 Overview

After the fast leave function is enabled, if a device receives an IGMP Leave packet of a specified group, the device directly deletes this interface from the group member records to shorten the leave latency.

1.10.2 Restrictions and Guidelines

This function applies to an interface that runs IGMPv2 or IGMPv3 and that is connected to only one host.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the fast leave function.

ip igmp immediate-leave group-list { *acl-name* | *acl-number* }

The fast leave function on an interface is disabled by default.

1.11 Configuring the Querier Robustness Variable

1.11.1 Overview

The querier robustness variable is used to calculate the aging time of a forwarding entry after a device receives an IGMP Report packet. Aging time = Query interval × Robustness variable + 10

1.11.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the querier robustness variable.

ip igmp robustness-variable *robustness-variable-number*

The default querier robustness variable is **2**.

1.12 Adding a Static Interface to a Group

In normal cases, an interface can join a multicast group only after the interface receives an IGMP Report packet from the multicast group.

If you manually add an interface to a group, the interface can be added to the group and exchanges multicast group information with the PIM router without IGMP packet exchange.

1.12.1 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Add a static interface to a group.

ip igmp static-group *group-address*

No static interface is added to a group by default.

1.13 Simulating a Host to Join a Group

1.13.1 Overview

By simulating a host to join a group, you can simulate host behaviors and send a Join packet to the upstream devices to join the group. This function is used to test the multicast function.

1.13.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Simulate a host to join a group.

ip igmp join-group *group-address*

The behavior of simulating a host to join a group is not performed by default.

1.14 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information of the **debug** command occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear ip igmp group	Clears dynamic group member records in the IGMP cache.
clear ip igmp interface *interface-type interface-number*	Clears all IGMP statistics and group member records on the interface.
show ip igmp groups [*interface-type interface-number*] [*group-address*] [**detail**]	Displays groups directly connected to the device and group information learned from IGMP.
show ip igmp interface [*interface-type interface-number*]	Displays IGMP configurations of the interface.
show ip igmp ssm-mapping [*group-address*]	Displays IGMP SSM mapping information.
show debugging	Displays the status of the IGMP debugging switch.
debug ip igmp all	Debugs all IGMP information.
debug ip igmp decode	Debugs IGMP packet resolution.
debug ip igmp encode	Debugs IGMP packet encoding.
debug ip igmp events	Debugs IGMP event information.
debug ip igmp fsm	Debugs IGMP Finite State Machine (FSM).
debug ip igmp tib	Debugs IGMP state machine information.
debug ip igmp warning	Debugs IGMP warning.

Contents

1 Configuring PIM-SM 1
1.1 Introduction 1
1.2 Principles 1
1.2.1 ASM Model 1
1.2.2 SSM Model 6
1.2.3 Protocols and Standards 7
1.3 Restrictions and Guidelines 8
1.4 Configuration Task Summary 8
1.5 Enabling the PIM-SM Function 8
1.5.1 Overview 8
1.5.2 Restrictions and Guidelines 9
1.5.3 Prerequisites 9
1.5.4 Procedure 9
1.6 Configuring PIM-SM in the ASM Model 9
1.6.1 Overview 9
1.6.2 Configuration Tasks 10
1.6.3 Prerequisites 10
1.6.4 Configuring a Static RP 10
1.6.5 Configuring C-BSRs and Related Parameters 11
1.6.6 Configuring C-RPs and Related Parameters 12
1.6.7 Configuring Registration Parameters 14
1.6.8 Configuring the Last Hop Device to Switch over from the RPT to SPT 17

1.7 Configuring PIM-SM in the SSM Model....18
1.7.1 Overview....18
1.7.2 Restrictions and Guidelines....18
1.7.3 Prerequisites....18
1.7.4 Procedure....18
1.8 Configuring PIM Neighbor Parameters....19
1.8.1 Overview....19
1.8.2 Configuration Tasks....19
1.8.3 Prerequisites....19
1.8.4 Configuring the Neighbor Message Time Parameters....19
1.8.5 Configuring Neighbor Tracking....20
1.8.6 Configuring Neighbor Filtering....20
1.9 Configuring DR Priority....21
1.9.1 Overview....21
1.9.2 Prerequisites....21
1.9.3 Procedure....21
1.10 Configuring Parameters of the Join/Prune Packets....21
1.10.1 Overview....21
1.10.2 Restrictions and Guidelines....21
1.10.3 Configuration Tasks....22
1.10.4 Prerequisites....22
1.10.5 Configuring Join/Prune Packet Sending Interval....22
1.10.6 Configuring the Prune Delay....22
1.11 Enabling PIM-SM on the Super VLAN Interface....23

1.12 Enabling PIM BFD Correlation 24

1.13 Monitoring 25

1.14 Configuration Examples..... 26

1.14.1 Configuring Basic Functions of PIM-SM in the ASM Model 26

1.14.2 Configuring Basic Functions of PIM-SM in the SSM Model 48

1 Configuring PIM-SM

1.1 Introduction

The Protocol Independent Multicast (PIM) is an intra-domain multicast routing protocol that is independent from unicast routing protocols. Any unicast routing protocol, for example, static route, Routing Information Protocol (RIP), and Open Shortest Path First (OSPF), can provide routing information for IP multicast. Multicast routing is independent from unicast routing, and simply uses unicast routing tables to generate multicast routing information. The Protocol Independent Multicast-Sparse Mode (PIM-SM) is used most widely, and applies to networks of any form, especially large networks where group members are scattered in a wide area. Compared with other intra-domain multicast routing protocols, PIM-SM has irreplaceable advantages.

1.2 Principles

PIM-SM considers that not all hosts need to receive multicast data, and sends multicast data to hosts that require the multicast data.

A PIM multicast device provides multicast service in any-source multicast (ASM) and source-specific multicast (SSM) models. For groups in the SSM address range, the SSM model is used. For other groups, the ASM model is used. In the ASM model, a host joins a specified multicast group G without the multicast source S specified. In the SSM model, a host can join a specified multicast group G to receive multicast data from a specified source S.

1.2.1 ASM Model

1. Basic Principles

PIM-SM in the ASM model is implemented as follows:

- A rendezvous point (RP) is used as a root of a rendezvous point tree (RPT) for transition. The designated router (DR) connected to a host sends a join message to the RP of a multicast group, and the multicast devices on the route create (*, G) entries hop by hop. Based on the entries, an RPT is created with the RP as the root.
- To send data to a multicast group, the source DR sends a register message to the RP to create an (S, G) entry on the RP. After the registration succeeds, the multicast source sends multicast data to the RP. After the multicast data arrives at the RP, it is copied and sent to the host via the RPT.

In the ASM model, the key mechanisms of PIM-SM include PIM neighbor creation, DR election, RP, bootstrap router (BSR), multicast source registration, shortest path tree (SPT) switchover, and assertion.

2. PIM Neighbor Creation

Neighbor relationship must be created between PIM multicast devices to form a PIM network, so that PIM control messages and multicast packets can be transmitted on the network. A Hello message is sent from a PIM interface. In the multicast packet with the Hello message encapsulated, the destination address is 224.0.0.13 (indicating all PIM multicast devices in the same network segment), the source address is the IP address of the PIM interface, and the time to live (TTL) value is 1. The Hello message is used to:

- Discover PIM neighbors.

PIM multicast devices in the same network segment receive the multicast packet with the destination address as 224.0.0.13, obtain neighbor information, and create neighbor relationship. After the neighbor relationship is created, the PIM interfaces can receive and process other PIM packets and create multicast routing entries.

When a PIM interface is enabled or detects a new neighbor, a Triggered-Hello-Delay message is used to generate a random time. Within the time, the interface sends Hello messages.

- Negotiate protocol parameters. The Hello message contains the following key parameters:
  - **DR Priority**: The priority of a multicast device for DR election. The device with a higher priority is selected.
  - **Holdtime**: The neighbor is considered reachable before timeout.
  - **Propagation Delay**: Duration between the time when a PIM device receives a prune packet and the time when the PIM device sends the prune packet to the uplink devices.
  - **Override-Interval**: The interval to override the prune.
- Maintain neighbor relationship.

  A Hello message is sent periodically between PIM multicast devices. If no new Hello message is received from a PIM neighbor within the hold time, this neighbor is considered unreachable and then removed from the neighbor list. Any change of PIM neighbors will cause change of the multicast topology in the network. If an uplink or a downlink neighbor in a multicast distribution tree (MDT) is unreachable, multicast routes converge again and the MDT is reshaped.

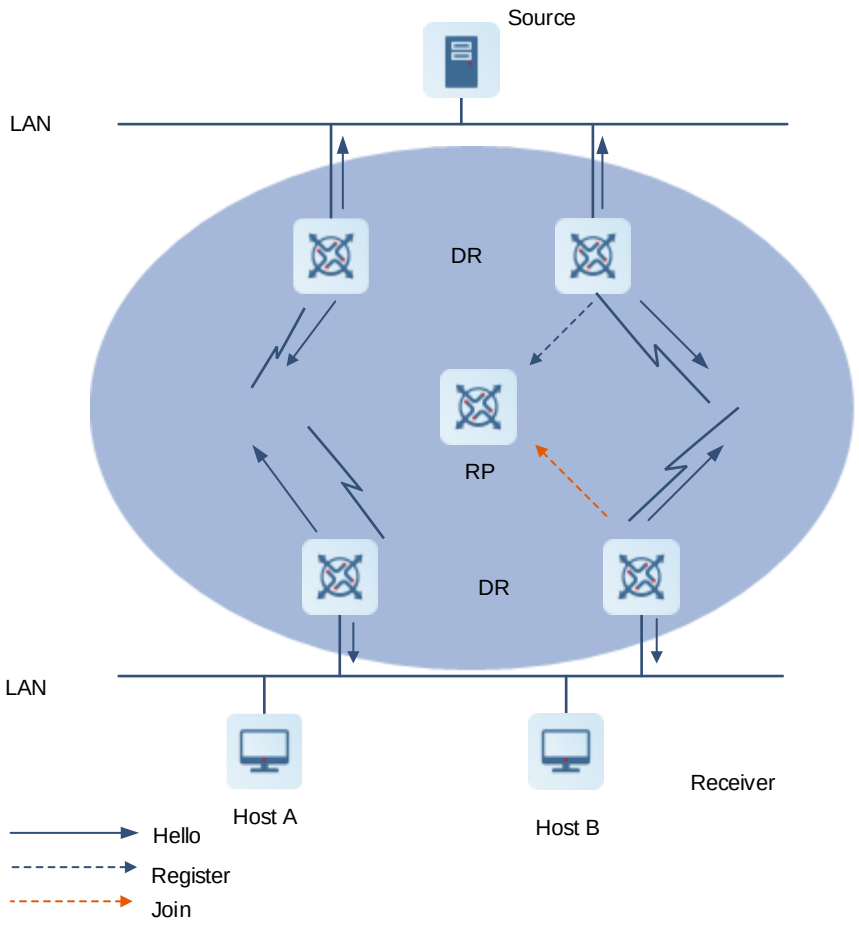
3. DR Election

As shown in Figure 1-1, the source DR sends a register message to the RP. Member DRs send join messages to the RP and forward multicast data to members in a multicast group. In the network segment to which members and multicast source are connected, multiple PIM devices obtain IP addresses and DR priorities of neighbors based on the Hello messages sent between the PIM devices during PIM neighbor creation. The PIM device that is elected becomes a member DR or source DR. The election rules are as follows:

(1) The DR priorities are compared. The device with a higher priority is selected.

(2) If the DR priorities are the same or there is any neighbor in the shared network segment that does not support DR priority, the IP addresses of the devices are compared. The device with a larger IP address is selected.

Figure 1-1 Schematic Diagram of DR Election



4. BSR Election

In the PIM network, the BSR periodically generates bootstrap messages (BSMs) that include a series of candidate-RPs (C-RPs) and corresponding group addresses. The BSMs are sent in the entire domain hop by hop. All PIM multicast devices in the network receive the BSMs and record the C-RPs and corresponding group addresses.

In the PIM-SM domain, one or multiple candidate-BSRs (C-BSRs) are configured and the BSR is elected based on rules.

5. RP Election

In the PIM network, the RP processes register messages of the source DR and join packets of group members. The process from the multicast source to members of the multicast group is divided into two sections: The SPT that uses the source DR as the root and the RP as the leaf, and the RPT that uses the RP as the root and member DRs as leaves. In the PIM-SM network with the ASM model, the RP must act as a transition to create or forward data.

In the PIM network, an RP can serve one or more groups, and a group can be served by only one RP. In the PIM network, the RP can be configured as static or dynamic.

- Static RP

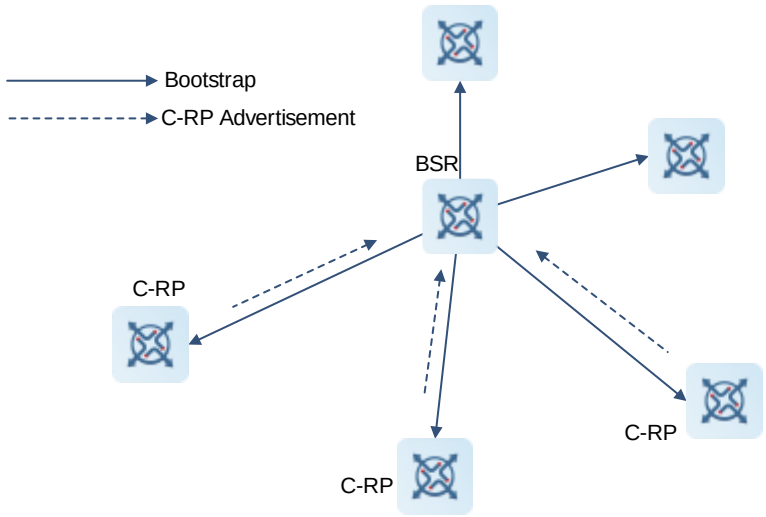
A static RP sets the RP address on each PIM multicast device to enable the entire PIM network to know the RP address.

- Dynamic RP

  As shown in Figure 1-2, multiple C-RPs can be configured in a PIM-SM domain to elect an RP dynamically. These C-RPs add their own addresses and served multicast groups to advertisement packets and sent the packets to the BSR periodically in unicast mode. The BSR is elected from the configured C-BSRs based on rules. The BSR periodically generates BSMs that include a series of C-RPs and corresponding group addresses. The BSMs are sent in the entire domain. Each PIM device in the domain receives and saves these BSMs, and applies the same hash algorithms to compute and elect an RP for each group. The BSR and RP election process is as follows:

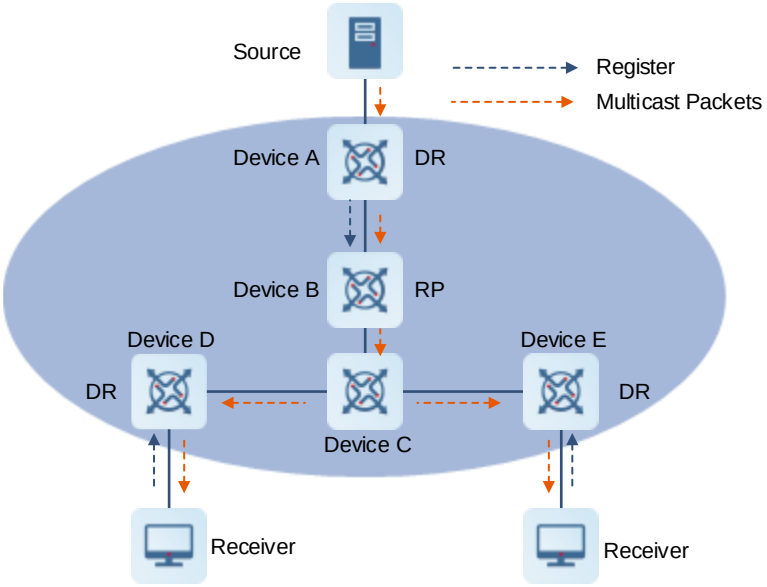
  - BSR election process: Initially, each C-BSR considers itself a BSR and sends a BSM throughout the network. The BSMs carry the C-BSR addresses and priorities. Upon receiving the BSMs, each PIM device compares the C-BSR addresses and priorities to elect the BSR.
  - RP election process: The C-RPs periodically send advertisement packets to the BSR in unicast mode to advertise the C-RP addresses, priorities, and addresses of the served groups. The BSR collects the information as RP-Set, encapsulates the information in a BSM, and sends the messages to each PIM device in the network. Upon receiving the RP-Set, the PIM devices in the network use the same algorithms for computation to obtain the RP that serves each group. Each PIM device obtains the RP position of each group.

Figure 1-2 Schematic Diagram of Dynamic RP Election



6. Multicast Source Registration

Figure 1-3 Schematic Diagram of Multicast Source Registration



As shown in Figure 1-3, when a multicast source sends data to a group, the source DR sends a register message to the RP so that the RP obtains the source information and a multicast packet and forwards the multicast packet to the members in the group. The forwarding process is as follows:

(1) The multicast source sends a multicast packet to the source DR.

(2) The source DR encapsulates the multicast packet in a register message and sends the message to the RP in unicast mode.

(3) Upon receiving the register message, the RP decapsulates the message and forwards the multicast packet to the members in a group via the RPT. Meanwhile, the RP sends an (S, G) join packet to the source. The PIM devices on the route create (S, G) entries, and finally create an SPT from the source to the RP.

(4) The source DR S forwards multicast packets based on this SPT. The multicast data is sent to the RP in the form of multicast packets.

(5) Upon receiving multicast packets from the source, the RP discards the register message and sends a register-stop message to the source.

(6) Upon receiving the register-stop message, the source DR stops encapsulating the register message, forwards multicast packets via the SPT, and periodically sends a register-probe message to the RP.

(7) Upon receiving the register-probe message, the RP sends a register-stop message to the source DR and updates the (S, G) entries.

(8) Upon receiving the register-stop message, the source DR continues forwarding multicast packets via the SPT without encapsulating the register message.

7. RPT Construction

When a group member joins the network, the DR connecting to the group member sends a join packet to the RP. If a multicast source has sent a multicast packet to the RP, the multicast packet will be sent to the group member via the RPT.

The RPT construction procedure is as follows:

- When a member DR receives an IGMP (*, G) INCLUDE Report packet, if the member DR is not an RP of the group G, the member DR sends a (*, G) join packet to the RP and the multicast devices on the route create the (*, G) entries hop by hop to generate an RPT that uses the RP as the root.
- During RPT construction, each PIM device checks the reverse path forwarding (RPF) when sending a join packet to the RP to find the unicast route to the RP. The outbound interface of the unicast route is an uplink interface, and the next hop of the unicast route is the RPF neighbor. The join packet is sent from the member DR to the RP.

8. SPT Switchover

In the PIM-SM network of the ASM model, one or multiple multicast groups correspond to one RP. Before SPT switchover, all packets of multicast groups sent to the RP service must be transitioned by the RP. When the sending rate of multicast packets grows, the RP load is increased. To solve this problem, the PIM-SM switches over the SPT to relieve the RP load. SPT switchover can be triggered by the RP or a member DR.

- SPT switchover triggered by the RP

  After receiving a register message from the source DR, the RP decapsulates the register message, forwards the multicast packets in the message to the group members via the RPT, and sends an (S, G) join packet to the source DR. The PIM multicast devices on the route create (S, G) entries hop by hop to create an SPT from the RP to the source.
- SPT switchover triggered by a member DR

  a When receiving the first multicast packet from the RP, the member DR obtains the source address.

  b The member DR sends an (S, G) join packet to the source. The PIM devices on the route create (S, G) entries and create an SPT from the member DR to the source DR.

  c After the SPT is created, the member DR sends a prune packet to the RP hop by hop and removes the downlink interface from the (*, G) entries. After the pruning, the RP does not forward multicast packets to the member DR via the RPT.

  d The SPT from the member DR to the source DR does not pass the RP. The RP sends a prune packet to the source DR to remove the downlink interface from the (S, G) entries. After the pruning, the source DR does not forward packets to the RP via the original "RP-source DR" SPT.

1.2.2 SSM Model

1. Basic Principles

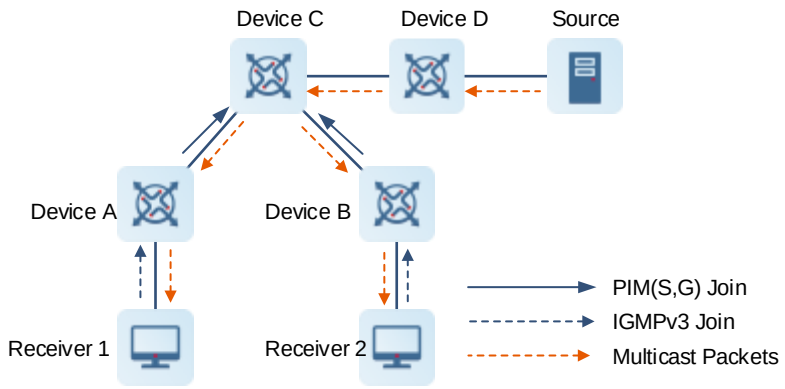
In the SSM model, members in a multicast group can specify to receive or reject data from a multicast source. The group members get to know the (S, G) entries of sources through access to the server or receiving advertisements. After understanding requirement of group members, the member DR sends a join packet to the source DR. This join packet is transmitted to the multicast source hop by hop to create an SPT from the source to the group members.

Note

- To implement the SSM model on IPv4, complete multicast interconnection through the PIM-SM and configure IGMPv3 to manage relationship between the hosts and devices.
- SSM model requirements: The hosts must know the addresses of multicast sources in advance using other network services so that the hosts can select multicast sources.

- On the devices that reside on the route from the hosts to the multicast source, the PIM-SM and SSM functions must be enabled.

Figure 1-4 SSM Model



Note

After the SSM function is enabled, the default group range of the SSM is **232/8**. You can modify the group range of the SSM using commands.

In the SSM model, the key mechanisms of PIM-SM include neighbor creation, DR election, and SPT creation.

2. PIM Neighbor Creation

For more information about the PIM neighbor creation mechanism in the SSM model, see the PIM neighbor creation mechanism in the ASM model in 1.2.1 2. PIM Neighbor Creation.

3. DR Election

For more information about the DR election mechanism in the SSM model, see the DR election mechanism in the ASM model in 1.2.1 3. DR Election.

4. SPT Construction

The SPT construction mechanism is as follows:

(1) The source DR learns through IGMPv3 that a group member wants to receive data of a multicast source and sends an (S, G) join packet to the source hop by hop.

(2) The PIM multicast devices on the route receive the (S, G) join packet and create the (S, G) entries, creating an SPT from the group member to the source.

(3) After the SPT is created, the multicast source distributes the multicast packets to the group member via the SPT.

1.2.3 Protocols and Standards

- RFC4601: Protocol Independent Multicast-Sparse Mode (PIM-SM)
- RFC5059: Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
- RFC3962: Protocol Independent Multicast-Dense Mode protocol

- RFC4607: Source-Specific Multicast for IP

1.3 Restrictions and Guidelines

- Before PIM-SM is enabled, enable the multicast routing and forwarding function in global configuration mode. Otherwise, multicast packets cannot be sent even if PIM-SM is enabled.
- In the IPv4 multicast network, the PIM (IPv4) protocol must be run on all L3 devices. Otherwise, a forwarding route cannot be created.

1.4 Configuration Task Summary

The PIM-SM configuration includes the following tasks:

(1) Enabling the PIM-SM Function

(2) Configuring a model for PIM-SM. Select at least one of the configuration tasks to complete.

- Configuring PIM-SM in the ASM Model
- Configuring PIM-SM in the SSM Model

(3) Configuring PIM Neighbor Parameters. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Neighbor Message Time Parameters
- Configuring Neighbor Tracking
- Configuring Neighbor Filtering

(4) (Optional) Configuring DR Priority

(5) Configuring Parameters of the Join/Prune Packets. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring Join/Prune Packet Sending Interval
- Configuring the Prune Delay

(6) (Optional) Enabling PIM-SM on the Super VLAN Interface

(7) (Optional) Enabling PIM BFD Correlation

1.5 Enabling the PIM-SM Function

1.5.1 Overview

Neighbor relationship must be created between PIM multicast devices to form a PIM-SM network, so that PIM control messages and multicast packets can be transmitted on the network. The PIM-SM function must be configured on all interfaces so that PIM neighbor creation, multicast entry creation, and multicast packet forwarding can be successful.

In a PIM network, if you want an interface, for example, a stub network device interface connecting to hosts, to receive multicast packets without involving the PIM network topology construction, you can set the interface to the PIM-SM passive mode. After the PIM-SM passive mode is configured, the interface does not process PIM packets. This improves device performance.

1.5.2 Restrictions and Guidelines

- The IPv4 multicast routing function must be enabled on each multicast device.
- The PIM-SM function should be enabled on the following interfaces: interfaces interconnecting multicast devices, interfaces connecting the static RP, C-RP and C-BSRs, and interfaces connecting multicast sources and hosts.
- PIM interfaces must be L3 interfaces, including: routing, L3AP, switch virtual interface (SVI), and loopback interfaces.

1.5.3 Prerequisites

All PIM interfaces can be reached via IPv4 unicast routes.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IPv4 multicast routing.

ip multicast-routing

The IPv4 multicast routing function is disabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Enable the PIM-SM function.

ip pim sparse-mode

The PIM-SM function is disabled by default.

(6) (Optional) Enable the PIM-SM passive mode.

ip pim sparse-mode passive

The PIM-SM passive mode is disabled by default.

1.6 Configuring PIM-SM in the ASM Model

1.6.1 Overview

The PIM-SM network supports the multicast service in the ASM and SSM models. Either one model or two models can be configured.

PIM-SM in the ASM model can provide hosts with multicast services of any source. A host joining a multicast group can receive multicast packets destined to this multicast group from any source.

If you require a PIM network to support the multicast service in the ASM model, an RP must be configured. There are three methods to configure an RP:

- Configure a static RP.
- Configure a dynamic RP.

- Configure static and dynamic RPs. If static and dynamic RPs are available at the same time, dynamic RPs are preferred.

1.6.2 Configuration Tasks

The PIM-SM ASM model configuration includes the following tasks. Select the tasks to configure a static RP or a dynamic RP, or configure both.

- Configuring a Static RP
- Configuring a Dynamic RP
  - Configuring C-BSRs and Related Parameters
  - Configuring C-RPs and Related Parameters
  - (Optional) Configuring Registration Parameters
- (Optional) Configuring the Last Hop Device to Switch over from the RPT to SPT

1.6.3 Prerequisites

In the PIM-SM multicast network, all nodes are reachable via IPv4 unicast routes.

1.6.4 Configuring a Static RP

1. Overview

You can manually configure a static RP to prevent frequent packet interaction between the BSR and C-RPs or between the BSR and PIM multicast devices and avoid bandwidth occupation. If the multicast network is simple or small, you can configure a static RP.

2. Restrictions and Guidelines

- Static RPs must be configured on every multicast device.
- The multicast device selected as a static RP must boast high performance.
- You are advised to use the loopback interface as a static RP address.
- Static RPs configured on multicast devices should be consistent, including RP address and address range of the served groups.
- If multiple static RPs are configured to correspond to different addresses of groups, the RPs can implement load balancing.
- If multiple static RPs serve the same group, the static RP with a larger IP address is selected first.
- You can use the control list to configure an RP to serve multiple (referencing an ACL) or all (not referencing an ACL) multicast groups. However, an RP can adopt only one configuration. The last configuration overrides the preceding configurations.

3. Prerequisites

Before an address range of a group is configured for an RP, ensure that the corresponding ACL is created and specify a multicast group range for the static RP to serve. For more information about ACL configuration, see *Configuring ACL*.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static RP.

ip pim rp-address *rp-address* [{ *acl-name* | *acl-number* }]

No static RP is configured by default.

1.6.5 Configuring C-BSRs and Related Parameters

1. Overview

In the PIM-SM domain of the ASM model, a unique BSR must be available. The BSR collects and releases RP information.

- The BSR is elected from C-BSRs based on rules. The election rules are as follows:
  - a The priorities of the C-BSRs are compared. The device with a higher priority is selected.
  - b If the priorities are the same, the IP addresses are compared. The device with a larger IP address is selected.
  - c The winner is elected as the BSR in the domain and periodically sends BSMs in the domain. A BSM contains the BSR IP address, RP-Set and hash mask information. The hash mask is used for hash calculation during C-RP election. In the hold time of a BSM, if other C-BSRs do not receive the BSM from the BSR, the BSR is considered unreachable and a new round of BSR election is initiated.
- To avoid fraud by an illegitimate BSR, a BSR range can be specified on all PIM devices in the domain so that the PIM devices ignore a BSM that is sent from an illegitimate BSR.
- To limit BSM flooding, you can configure a BSR border on an interface. Upon receiving BSMs, this interface discards the BSMs without forwarding them. This limits the BSM flooding.

2. Restrictions and Guidelines

- C-BSRs must be configured on one or multiple multicast devices.
- The multicast devices selected as C-BSRs must boast high performance. The C-RPs and C-BSRs can reside on the same or different multicast devices.
- You are advised to use the loopback interface as a C-BSR address.
- If multiple C-BSRs are configured, they can implement redundancy backup.
- You are advised to configure a valid BSR address range on all PIM devices in the domain.
- A BSR border must be configured on the interface between domains.

3. Prerequisites

- Enabling the PIM-SM Function.
- Before a valid BSR address range is configured on PIM devices, ensure that the corresponding ACL is created and specify a valid BSR range. For more information about ACL configuration, see *Configuring ACL*.

4. Procedure

(1) Configure C-BSRs and related parameters.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Configure C-BSRs.

ip pim bsr-candidate *interface-type interface-number* [*hash-mask-length* [*priority-value*]]

No C-BSR is configured by default.

(2) (Optional) Configure a valid BSR address range on all PIM devices.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Configure a BSM limit on the PIM multicast devices.

ip pim accept-bsr list { *acl-name* | *acl-number* }

All BSMs are received by default.

(3) (Optional) Configure a BSR border on the interface between PIM-SM domains.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Enter the interface configuration mode.

interface *interface-type interface-number*

d Configure a BSR border.

ip pim bsr-border

No BSR border is configured by default.

If multiple domains exist, the BSR border must be configured on the interface between two domains.

1.6.6 Configuring C-RPs and Related Parameters

1. Overview

- After a multicast device is configured as a C-RP, the C-RP periodically sends an advertisement packet to the BSR in unicast mode. The packet includes the RP priority, advertisement packet hold time (greater than the interval of sending the advertisement packet), RP address, address of the served group, and prefix of the multicast address. Upon receiving the advertisement packet, the BSR collects the information in the packet as RP-Set in the advertisement packet hold time, encapsulates the information in a BSM, and sends the message to all PIM devices. Upon receiving the BSM from the BSR, the PIM devices in the domain apply the same algorithms for hash calculation to calculate the C-RP serving each multicast group. After the advertisement packet hold timer times out, if the BSR does not receive a next advertisement packet from the C-RP, this C-RP is considered unreachable.
- To prevent fraud by an illegitimate C-RP, a C-RP range can be specified on the BSR. If an advertisement packet comes from an illegitimate C-RP, the packet is ignored.

- The BSR can determine whether to receive an advertisement packet with the prefix of the multicast address being 0 from a C-RP. When the prefix of the multicast address is 0, this C-RP serves all multicast groups.
- When receiving the BSM from the BSR, each PIM multicast device in the domain applies rules to select the RP. The RP election rules are as follows:
  - a The address of the multicast group that a host joins is compared with the mask length of the group address range that the C-RP serves. The device with the longest mask is selected.
  - b If the addresses are consistent with the mask length, the priorities of the C-RPs are compared. The device with the smallest priority value is selected.
  - c If the priorities are consistent, hash values are calculated and compared. The device with the largest hash value is selected.
  - d If the hash values are the same, the IP addresses of the C-RPs are compared. The device with the largest IP address is selected.

2. Restrictions and Guidelines

- C-RPs must be configured on one or multiple multicast devices.
- The multicast devices selected as C-RPs must boast high performance. The C-RPs and C-BSRs can reside on the same or different multicast devices.
- You are advised to use the loopback interface as a C-RP address.
- If multiple C-RPs are configured to serve the same group, they can implement redundancy backup.
- If multiple C-RPs are configured to serve different groups, they can implement load balancing.
- A valid C-RP range can be configured on the BSR.
- To specify a group range for C-RPs to serve, you can add the ACL option to the **ip pim rp-candidate** command. The group range is calculated based on the permit access control entry (ACE), rather than the deny ACE.

3. Prerequisites

- Enabling the PIM-SM Function.
- If the **group-list** parameter is used to limit the range of groups served by the RP, ensure that the corresponding ACL is created and specify a multicast group range for the RP to serve. For more information about ACL configuration, see *Configuring ACL*.

4. Procedure

- Configure C-RPs and related parameters.
  - a Enter the privileged EXEC mode.

    enable
  - b Enter the global configuration mode.

    configure terminal
  - c Configure C-RPs.

    ip pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval*] [**group-list** { *acl-name* | *acl-number* }]

    No C-RP is configured by default.

- (Optional) Configure the BSR to receive C-RP advertisement packets with the prefix of the multicast address being 0. This C-RP serves all the multicast groups.

  a Enter the privileged EXEC mode.

  enable

  d Enter the global configuration mode.

  configure terminal

  e Configure the BSR to receive advertisement packets from the C-RP that serves all multicast groups.

  ip pim accept-crp-with-null-group

  The function for the BSR to receive advertisement packets from the C-RP that serves all multicast groups is disabled by default.

  You are advised to enable this function on all C-BSRs.

- (Optional) Configure a valid C-RP range on the BSR.

  a Enter the privileged EXEC mode.

  enable

  f Enter the global configuration mode.

  configure terminal

  g Configure a valid C-RP range.

  ip pim accept-crp list { *acl-name* | *acl-number* }

  The C-BSRs receive all external C-RP advertisement packets by default.

  You are advised to enable this function on all C-BSRs.

- (Optional) Configure to ignore RP priority on all PIM multicast devices and reselect an RP.

  a Enter the privileged EXEC mode.

  enable

  h Enter the global configuration mode.

  configure terminal

  i Configure to ignore the RP priority for RP election.

  ip pim ignore-rp-set-priority

  If the address of the multicast group that a host joins is consistent with the mask length of the group address range that the C-RPs serve, the RP with the highest priority is selected by default.

  You can configure to ignore C-RP priority on each multicast device.

1.6.7 Configuring Registration Parameters

1. Overview

When a multicast source sends multicast data, the data arrives at the source DR first. Upon receiving the multicast data, the source DR encapsulates the multicast data as a register message and sends the message to the RP. Related parameters of the register message are configured on the source DR and RP.

- You can configure the following parameters on the source DR:
  - RP reachability checking: Before sending a register message, the source DR determines whether the

RP is reachable. If the RP is reachable, the message is sent. Otherwise, the message is not sent.

- Limit on the rate of sending the register message: The rate of sending each register message in (S, G) status is limited. If multiple register messages in (S, G) status are sent from the same source, the rate of the register messages is limited to the product of *N* × Limit value.
- Source address in the register message: The source address in the register message is the address of the DR interface connected to the multicast source by default. If a security policy is configured on the RP to filter out this address, the RP does not receive register messages from this source DR. In this case, you can specify a reachable source address as the source address of the register message.
- Register suppression time: When the RP receives multicast packets sent by the multicast source via the SPT, the RP sends a register-stop message to the source DR. Within the register- suppression time, the source DR stops encapsulating the register message and sends multicast packets to the RP via the SPT. After the register suppression timer times out, if the source DR does not receive another register-stop message from the RP, the source DR continues to encapsulate the register message and send the message to the RP.
- Null message detection time: Before the register suppression timer times out, the RP receives a null message from the source DR, refreshes the local (S, G) entries, and sends a register-stop message to the source DR so that the source DR refreshes the register suppression timer. Otherwise, the source DR continues to encapsulate the register message and send multicast packets to the RP in the form of the register message.

- You can configure the following parameters on the RP:
  - (S, G) address range of source: Provide multicast services for hosts in the permitted multicast group in the ASM model. After this parameter is configured, the RP replies a register-stop message upon receiving data from an unauthorized source.
  - Length of register message checksum: Adjust the calculation method of the register message checksum and calculate the checksum of the entire PIM protocol packets (including encapsulated multicast packets) or the checksum of PIM headers of separate register messages.
  - Register message decapsulation and delivery to downlink interface: Configure this parameter on the RP to decapsulate the received register message and forward the multicast packets in the register message.
  - Register message (S, G) entry timeout period: Configure this parameter to configure the timeout period of (S, G) entries. The (S, G) entries age if no packet is received within the register message timeout period.

2. Restrictions and Guidelines

- The source address in the specified register message must be reachable in unicast mode. You are advised to use the loopback interface of the source DR as the source address of the register message.
- If the **ip pim rp-register-kat** command is not configured, modifying the register suppression time on the RP changes the (S, G) entry timeout period.
- Configuring a limit to the register message rate reduces the load of the source DR and RP. Only register messages under the limit are sent.
- The register-probe time cannot be greater than a half of the register suppression time. Otherwise, the configuration failed and an alarm is generated.

- The sum of the three times of register suppression time and the register-probe time does not exceed 65,535. Otherwise, the configuration failed and an alarm is generated.

3. Prerequisites

- Enabling the PIM-SM Function.
- Before an (S, G) address range is configured for the source, if the **list** parameter is specified, ensure that the corresponding ACL is created and specify an (S, G) address range for the source. For more information about ACL configuration, see *Configuring ACL*.
- Before an (S, G) address range is configured for the source, if the **route-map** parameter is specified, ensure that the corresponding route map is created and specify an (S, G) address range for the source. For more information about route map configuration, see *Configuring Route Policies*.
- Before the register message checksum calculation is applied to entire packets, if the **group-list** parameter is specified, ensure that the corresponding ACL is created and specify the register message checksum calculation to apply to the entire packets in a multicast group address range. For more information about ACL configuration, see "Configuring ACL" in *ACL and QoS Configuration Guide*.

4. Procedure

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configure registration parameters on the source DR.

  a Enter the privileged EXEC mode.

  enable

  b Enter the global configuration mode.

  configure terminal

  c Enable RP reachability checking on the source DR.

  ip pim register-rp-reachability

  The RP reachability checking function is disabled by default.

  d Limit the rate of sending register messages on the source DR.

  ip pim register-rate-limit *rate*

  The sending rate of register messages is not limited by default.

  e Configure a source address in the register messages on the source DR.

  ip pim register-source { *local-address* | *interface-type interface-number* }

  The source IP address in the register messages is the address of the DR interface connected to the source by default.

  f Configure the register suppression time on the source DR.

  ip pim register-suppression *suppression-time*

  The default register suppression time is **60** seconds.

  g Configure the null message detection time on the source DR.

  ip pim probe-interval *interval*

  The default register-probe time is **5** seconds.

- Configure registration parameters on the RP.

a Enter the privileged EXEC mode.

enable

h Enter the global configuration mode.

configure terminal

i Configure the (S, G) address range for the source on the RP.

ip pim accept-register { **list** { *acl-name* | *acl-number* } | **route-map** *route-map-name* } *

The (S, G) address range of register messages is not limited by default. The RP receives register messages of all (S, G) addresses.

j Enable register message checksum calculation to be applied to the entire packets on the RP.

ip pim register-checksum-wholepkt [**group-list** { *acl-name* | *acl-number* }]

By default, the register message checksum of headers of only PIM packets and register messages, rather than the entire packets, is calculated.

If the **group-list** parameter is not specified, this configuration applies to all group addresses.

k Enable the RP to decapsulate the received register messages and forward the multicast packets in the received register messages on the RP.

ip pim register-decapsulate-forward

The function for the RP to decapsulate the register messages and forward the multicast packets is disabled by default.

The register message decapsulation and multicast packet forwarding function is implemented by the corresponding software. If there are too many register messages to be decapsulated and forwarded, the CPU is overloaded. Therefore, you are not advised to enable this function.

l Configure the timeout period for the (S, G) entries created upon receiving the register message on the RP.

ip pim rp-register-kat *interval*

By default, the timeout period for the (S, G) entries is the sum of three times of the register suppression time and the register-probe time.

1.6.8 Configuring the Last Hop Device to Switch over from the RPT to SPT

1. Overview

If the multicast traffic in a network is heavy, the RP easily gets overloaded and then faulty. To relieve the RP load, you can initiate SPT switchover through the member DR. You can specify multicast groups to perform SPT switchover.

2. Prerequisites

- Enabling the PIM-SM Function.
- Before an address range of a group is configured for SPT switchover, ensure that the corresponding ACL is created and specify a multicast group range for SPT switchover. For more information about ACL configuration, see "Configuring ACL" in *ACL and QoS Configuration Guide*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the SPT switchover function.

ip pim spt-threshold [**group-list** { *acl-name* | *acl-number* }]

The SPT switchover function is disabled by default.

If the **group-list** parameter is not specified, all groups support SPT switchover.

1.7 Configuring PIM-SM in the SSM Model

1.7.1 Overview

The PIM-SM function in the SSM model can provide specified source services for hosts so that the hosts can determine to receive or reject multicast data of specified sources based on needs.

1.7.2 Restrictions and Guidelines

- If you require a PIM network to support the multicast service in the SSM model, the SSM function must be enabled.
- The SSM function must be enabled on each multicast device.
- The address range of SSM groups configured on all multicast devices must be consistent.
- IGMPv3 or SSM mapping must be enabled.

1.7.3 Prerequisites

- In the multicast network, all nodes are reachable via IPv4 unicast routes.
- Enabling the PIM-SM Function.
- Before an SSM group range is configured using an ACL, ensure that the corresponding ACL is created and specify an SSM multicast group range. For more information about ACL configuration, see "Configuring ACL" in *ACL and QoS Configuration Guide*.

1.7.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the SSM function.

ip pim ssm { **default** | **range** { *acl-name* | *acl-number* } }

The SSM function is disabled by default.

1.8 Configuring PIM Neighbor Parameters

1.8.1 Overview

PIM multicast devices transmit hello messages to discover neighbors, coordinate protocol parameters and maintain neighbor relationships.

1.8.2 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Neighbor Message Time Parameters
- Configuring Neighbor Tracking
- Configuring Neighbor Filtering

1.8.3 Prerequisites

- In the multicast network, all nodes are reachable via IPv4 unicast routes.
- Enabling the PIM-SM Function.

1.8.4 Configuring the Neighbor Message Time Parameters

1. Overview

The neighbor message time parameters include hello message sending interval and hello message sending delay.

- The hello message sending interval can be configured, and the hello message hold time is 3.5 times the hello message sending interval. If no new hello message is received within the hello message hold time, the neighbor is considered unreachable.
- When the PIM interface is enabled or detects a new neighbor, random time is generated and it is referred to as hello message sending delay. Within the delay time, the interface sends hello messages out.

2. Restrictions and Guidelines

If the hello message hold time is greater than 65,535 seconds, the hello message sending interval is automatically set to 18,725 seconds.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the neighbor message time parameters. Select at least one of them to configure.

- Configure the hello message sending interval.

  ip pim query-interval *interval*

  The hello message is sent at an interval of **30** seconds by default.

- Configure the hello message sending delay.

  ip pim triggered-hello-delay *delay*

  The hello message sending delay is **5** seconds by default.

1.8.5 Configuring Neighbor Tracking

1. Overview

After the suppression capability of an interface is enabled, when a multicast device plans to send a join packet to an uplink multicast device but it receives a join packet sent from the neighbor to the uplink multicast device, this local multicast device suppresses its own join packet. If the suppression capability of the interface is disabled, the join packet can be sent. When the suppression capability of downlink hosts is disabled, an uplink device can determine the number of the downlink hosts based on the quantity of received join packets. This is neighbor tracking.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the neighbor tracking function.

ip pim neighbor-tracking

The neighbor tracking function is disabled by default.

1.8.6 Configuring Neighbor Filtering

1. Overview

The neighbor filtering function can protect neighborhood. Controlling neighbors can strengthen PIM network security and limit the valid address range of neighbors. If a neighbor is filtered out based on an access filtering list, PIM-SM does not create peer relationship with the neighbor or stops the peer relationship with this neighbor.

2. Prerequisites

Before an access filtering list is configured, ensure that the corresponding ACL is created and specify a valid neighbor address range. For more information about ACL configuration, see "Configuring ACL" in *ACL and QoS Configuration Guide*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the neighbor filtering function.

ip pim neighbor-filter { *acl-name* | *acl-number* }

The neighbor filtering function is disabled by default.

1.9 Configuring DR Priority

1.9.1 Overview

In a network segment shared by multicast sources and group members, multiple PIM multicast devices exist. The PIM multicast devices elect a DR based on neighbor messages. A device with the highest priority is selected. If the priorities are the same or some PIM devices do not support the DR priority function, the IP addresses are compared and the PIM multicast device with the largest IP address is selected. The selected PIM device functions as a DR, transmits protocol packets between the sources and members, and forwards multicast packets.

1.9.2 Prerequisites

- In the multicast network, all nodes are reachable via IPv4 unicast routes.
- Enabling the PIM-SM Function.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a DR priority in hello messages.

ip pim dr-priority *priority-value*

The default DR priority in hello messages is **1**.

1.10 Configuring Parameters of the Join/Prune Packets

1.10.1 Overview

A device sends a join packet to request an uplink device to forward multicast packets and sends a prune packet to request the uplink device to stop forwarding multicast packets. The request route is referred to as an RPT or SPT.

1.10.2 Restrictions and Guidelines

- The network administrator must ensure that the prune override interval is smaller than the join-prune packet hold time. Otherwise, a short interrupt may occur.

- When the PIM multicast device receives a prune message from an uplink interface, there are other downlink devices existent in the shared network segment. If this PIM multicast device still needs to receive multicast data, the PIM multicast device must send a prune override message to the uplink device within the override interval.

1.10.3 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring Join/Prune Packet Sending Interval
- Configuring the Prune Delay

1.10.4 Prerequisites

Enabling the PIM-SM Function.

1.10.5 Configuring Join/Prune Packet Sending Interval

1. Overview

A PIM device periodically sends the join/prune packet to an uplink device to update the forwarding status. The join packet is used to request data forwarding and the prune packet is used to stop data forwarding. Upon receiving the join/prune packet, the uplink device starts the join/prune packet hold time timer.

- If a join packet hold time timer times out, the PIM device is suppressed to forward multicast packets of the corresponding multicast group through the downlink interface.
- If a prune packet hold time timer times, the PIM device is restored to forward the multicast packets of the corresponding multicast group through the downlink interface.

2. Restrictions and Guidelines

The join/prune packet sending interval must be smaller than the join/prune packet hold time. Generally, the join/prune packet hold time is 3.5 times the join/prune packet sending interval.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the join/prune packet sending interval.

ip pim jp-timer *interval*

The join/prune packet is sent at an interval of **60** seconds by default.

1.10.6 Configuring the Prune Delay

1. Overview

Upon receiving a prune packet from a downlink device, the multicast device does not perform prune immediately and it waits for a period of time. This period of time is divided into two parts: The part from the time when the multicast device receives a prune message to the time when the multicast device sends the prune message to the uplink device is referred to as the prune propagation delay; the part from the time when the PIM

device receives a prune packet to the time when the device continues to forward the multicast packets to a downlink device is referred to as the override interval. The period from the time when the multicast device receives a prune message to the time when the prune action is performed is the sum of the propagation delay and the override interval.

2. Restrictions and Guidelines

In the period from the time when the multicast device receives a prune message to the time when the prune action is performed, if the PIM device receives a prune override message from the downlink interface, the PIM device cancels pruning.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the prune message propagation delay.

ip pim propagation-delay *propagation-delay*

The default propagation delay of an interface is **500** ms.

(5) Configure the prune override interval.

ip pim override-interval *override-interval*

The default override interval is **2500** ms.

1.11 Enabling PIM-SM on the Super VLAN Interface

1. Overview

In most scenarios of a PIM network, the PIM-SM protocol does not need to be enabled on a super VLAN interface. A super VLAN interface is connected to many sub VLANs. If the PIM-SM protocol is enabled on the super VLAN interface, the device replicates and sends a multicast protocol packet to all the sub VLANs, which easily surpasses the processing capability of the device and causes packet loss even protocol flapping. In some scenarios, the PIM-SM protocol must be enabled on the super VLAN interface. You can configure the command to enable the protocol packets to be sent to the specified sub VLANs or all sub VLANs. If the packets are sent to all VLANs, protocol flapping may occur.

2. Restrictions and Guidelines

- This function must be enabled on the super VLAN interface.
- If you enable protocol packets to be sent to all sub VLANs, the packets may surpass the processing capability of the device, causing protocol flapping.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable PIM-SM protocol packets to be sent to specified sub VLANs.

ip pim sparse-mode subvlan [**all** | *vlan-id*]

The PIM-SM function is disabled on a super VLAN interface by default.

1.12 Enabling PIM BFD Correlation

1. Overview

In some shared multicast networks, PIM neighbor status change triggers re-initiation of some mechanisms, for example, DR election mechanism. Generally, a PIM neighbor triggers a new round of election after the neighborhood times out, causing multicast data interruption. PIM bidirectional forwarding detection (BFD) correlation can quickly detect link status and neighbor faults in a shared network segment and trigger a new round of DR election. This reduces multicast data transmission interrupt time and ensures reliability of the multicast network.

2. Restrictions and Guidelines

- If DR election or assertion election is required in a multicast network, you are advised to enable PIM-SM BFD correlation.
- The PIM BFD function must be enabled on the interconnection interface of the multicast devices.
- PIM interfaces must be L3 interfaces, including: routing, L3AP, switch virtual interface (SVI), and loopback interfaces.

3. Prerequisites

- In the network, all nodes are reachable via IPv4 unicast routes.
- Enabling the PIM-SM Function.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable PIM BFD correlation.

ip pim bfd

PIM BFD correlation is disabled by default.

1.13 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear ip mroute { * | *group-address* [*source-address*] }	Clears multicast routing entries.
clear ip mroute statistics { * | *group-address* [*source-address*] }	Clears statistical information about multicast routing.
clear ip pim sparse-mode bsr rp-set *	Clears dynamic RP information.
clear ip pim sparse-mode track	Clears statistical information about PIM-SM protocol packets.
show ip pim sparse-mode bsr-router	Displays details about the BSR.
show ip pim sparse-mode interface [*interface-type interface-number*] [**detail**]	Displays PIM-SM information of an interface.
show ip pim sparse-mode local-members [*interface-type interface-number*]	Displays local IGMP information about a PIM-SM interface.
show ip pim sparse-mode mroute [*group-or-source-address* [*group-or-source-address*]]	Displays information about the PIM-SM multicast routing table.
show ip pim sparse-mode neighbor [**detail**]	Displays PIM-SM neighbor information.
show ip pim sparse-mode nexthop	Displays the PIM-SM next hop information in an NSM.
show ip pim sparse-mode rp-hash *group-address*	Displays RP information corresponding to a group address.
show ip pim sparse-mode rp mapping	Displays all RPs and the groups served by the RPs.
show ip pim sparse-mode track	Displays the number of PIM packets sent and received since the statistic start time.

1.14 Configuration Examples

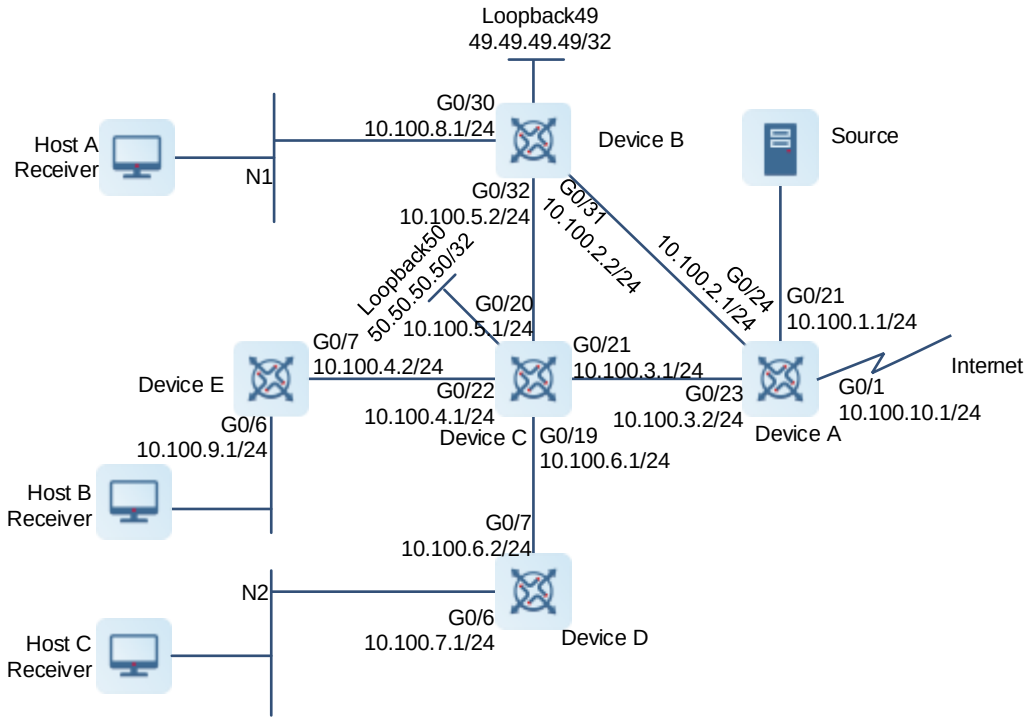
1.14.1 Configuring Basic Functions of PIM-SM in the ASM Model

1. Requirements

As shown in Figure 1-5, the internal network is connected to the Internet. The PIM-SM protocol is configured on each multicast device to provide ASM multicast services for hosts in networks N1 and N2 so that hosts joining a multicast group can receive multicast data destined to this multicast group from any multicast source, including video-on-demand information.

2. Topology

Figure 1-5 PIM-SM Multicast Network Topology in the ASM Model



3. Notes

- Configure IP addresses and unicast routing protocols for multicast devices. The PIM routing protocol in a multicast domain depends on unicast routing protocols. Normal communication of unicast routing lays a foundation of multicast routing. Ensure that each PIM node is reachable via unicast routes.
- Enable the multicast function on all multicast devices. Enabling the multicast function is a prerequisite of PIM-SM configuration.
- Enable the basic functions of PIM-SM on all interfaces of the multicast devices. The other functions of PIM-SM can be enabled only after the basic functions of PIM-SM are enabled.
- Enable the IGMP function on the interface connected to hosts so that the hosts can join or leave a multicast group by sending IGMP messages. The multicast devices acting as leaf nodes maintain group membership based on the IGMP protocol.

- Configure RPs. In the PIM-SM network in the ASM model, the RP is a transitional station for forwarding multicast data. It is recommended that the multicast device with many traffic flows be configured as an RP, for example, device C in Figure 1-5.
- Configure a BSR border on the interface connected to the Internet. BSMs must be transmitted in the PIM-SM domain within the border to improve the multicast controllability.

4. Procedure

(1) Configure IP addresses and enable unicast routing protocols on interfaces of different devices.

Configure IPv4 addresses on interfaces of device A, and configure the OSPF protocol to implement internetworking.

```
DeviceA> enable
DeviceA# config terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no switchport
DeviceA(config-if-GigabitEthernet 0/1)# ip address 10.100.10.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# no switchport
DeviceA(config-if-GigabitEthernet 0/21)# ip address 10.100.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/21)# exit
DeviceA(config)#interface gigabitEthernet 0/23
DeviceA(config-if-GigabitEthernet 0/23)# no switchport
DeviceA(config-if-GigabitEthernet 0/23)# ip address 10.100.3.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/23)# exit
DeviceA(config)# interface gigabitEthernet 0/24
DeviceA(config-if-GigabitEthernet 0/24)# no switchport
DeviceA(config-if-GigabitEthernet 0/24)# ip address 10.100.2.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/24)# exit
DeviceA(config)# router ospf 49
DeviceA(config-router)# network 10.100.1.0 0.0.0.255 area 0
DeviceA(config-router)# network 10.100.10.0 0.0.0.255 area 0
DeviceA(config-router)# network 10.100.2.0 0.0.0.255 area 0
DeviceA(config-router)# network 10.100.3.0 0.0.0.255 area 0
DeviceA(config-router)# exit
```

Configure IPv4 addresses on interfaces of device B, and configure the OSPF protocol to implement internetworking.

```
DeviceB> enable
DeviceB# config terminal
DeviceB(config)# interface GigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# no switchport
DeviceB(config-if-GigabitEthernet 0/30)# ip address 10.100.8.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface GigabitEthernet 0/31
DeviceB(config-if-GigabitEthernet 0/31)# no switchport
DeviceB(config-if-GigabitEthernet 0/31)# ip address 10.100.2.2 255.255.255.0
```

```
DeviceB(config-if-GigabitEthernet 0/31)# exit
DeviceB(config)# interface GigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# no switchport
DeviceB(config-if-GigabitEthernet 0/32)# ip address 10.100.5.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface loopback 49
DeviceB(config-if-Loopback 49)# ip address 49.49.49.49 255.255.255.255
DeviceB(config-if-Loopback 49)# exit
DeviceB(config)# router ospf 49
DeviceB(config-router)# network 10.100.8.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.2.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.5.0 0.0.0.255 area 0
DeviceB(config-router)# network 49.49.49.49 0.0.0.0 area 0
DeviceB(config-router)# exit
```

Configure IPv4 addresses on interfaces of device C, and configure the OSPF protocol to implement internetworking.

```
DeviceC> enable
DeviceC# config terminal
DeviceC(config)# interface GigabitEthernet 0/19
DeviceC(config-if-GigabitEthernet 0/19)# no switchport
DeviceC(config-if-GigabitEthernet 0/19)# ip address 10.100.6.1 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/19)# exit
DeviceC(config)#interface GigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# no switchport
DeviceC(config-if-GigabitEthernet 0/20)# ip address 10.100.5.1 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# no switchport
DeviceC(config-if-GigabitEthernet 0/21)# ip address 10.100.3.1 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface GigabitEthernet 0/22
DeviceC(config-if-GigabitEthernet 0/22)# no switchport
DeviceC(config-if-GigabitEthernet 0/22)# ip address 10.100.4.1 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/22)# exit
DeviceC(config)# interface loopback 50
DeviceC(config-if-Loopback 50)# ip address 50.50.50.50 255.255.255.255
DeviceC(config-if-Loopback 50)# exit
DeviceC(config)# router ospf 49
DeviceC(config-router)# network 10.100.6.0 0.0.0.255 area 0
DeviceC(config-router)# network 10.100.5.0 0.0.0.255 area 0
DeviceC(config-router)# network 10.100.3.0 0.0.0.255 area 0
DeviceC(config-router)# network 10.100.4.0 0.0.0.255 area 0
DeviceC(config-router)# network 50.50.50.50 0.0.0.0 area 0
DeviceC(config-router)# exit
```

Configure IPv4 addresses on interfaces of device D, and configure the OSPF protocol to implement internetworking.

```
DeviceD> enable
DeviceD# config terminal
DeviceD(config)# interface GigabitEthernet 0/6
DeviceD(config-if-GigabitEthernet 0/6)# no switchport
DeviceD(config-if-GigabitEthernet 0/6)# ip address 10.100.7.1 255.255.255.0
DeviceD(config-if-GigabitEthernet 0/6)# exit
DeviceD(config)# interface GigabitEthernet 0/7
DeviceD(config-if-GigabitEthernet 0/7)# no switchport
DeviceD(config-if-GigabitEthernet 0/7)# ip address 10.100.6.2 255.255.255.0
DeviceD(config-if-GigabitEthernet 0/7)# exit
DeviceD(config)# router ospf 49
DeviceD(config-router)# network 10.100.6.0 0.0.0.255 area 0
DeviceD(config-router)# network 10.100.7.0 0.0.0.255 area 0
DeviceD(config-router)# exit
```

Configure IPv4 addresses on interfaces of device E, and configure the OSPF protocol to implement internetworking.

```
DeviceE> enable
DeviceE# config terminal
DeviceE(config)# interface GigabitEthernet 0/6
DeviceE(config-if-GigabitEthernet 0/6)# no switchport
DeviceE(config-if-GigabitEthernet 0/6)# ip address 10.100.9.1 255.255.255.0
DeviceE(config-if-GigabitEthernet 0/6)# interface GigabitEthernet 0/7
DeviceE(config-if-GigabitEthernet 0/7)# no switchport
DeviceE(config-if-GigabitEthernet 0/7)# ip address 10.100.4.2 255.255.255.0
DeviceE(config-if-GigabitEthernet 0/7)# exit
DeviceE(config)# router ospf 49
DeviceE(config-router)# network 10.100.9.0 0.0.0.255 area 0
DeviceE(config-router)# network 10.100.4.0 0.0.0.255 area 0
DeviceE(config-router)# exit
```

(2) Enable the multicast and PIM-SM functions on all multicast devices, and enable the IGMP function on all multicast devices connected to hosts.

Enable the multicast and PIM-SM functions on device A.

```
DeviceA(config)# ip multicast-routing
DeviceA(config)# interface gigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/21)# exit
DeviceA(config)# interface gigabitEthernet 0/23
DeviceA(config-if-GigabitEthernet 0/23)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/23)# exit
DeviceA(config)# interface gigabitEthernet 0/24
DeviceA(config-if-GigabitEthernet 0/24)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/24)# exit
```

Enable the multicast, PIM-SM, and IGMP functions on device B.

```
DeviceB(config)# ip multicast-routing
```

```
DeviceB(config)# interface gigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# ip pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface gigabitEthernet 0/31
DeviceB(config-if-GigabitEthernet 0/31)# ip pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/31)# exit
DeviceB(config)# interface gigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# ip pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface loopback 49
DeviceB(config-if-Loopback 49)# ip pim sparse-mode
DeviceB(config-if-Loopback 49)# exit
```

Enable the multicast and PIM-SM functions on device C.

```
DeviceC(config)# ip multicast-routing
DeviceC(config)# interface gigabitEthernet 0/19
DeviceC(config-if-GigabitEthernet 0/19)# ip pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/19)# exit
DeviceC(config)# interface gigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# ip pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface gigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# ip pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface gigabitEthernet 0/22
DeviceC(config-if-GigabitEthernet 0/22)# ip pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/22)# exit
DeviceC(config)# interface loopback 50
DeviceC(config-if-Loopback 50)# ip pim sparse-mode
DeviceC(config-if-Loopback 50)# exit
```

Enable the multicast, PIM-SM, and IGMP functions on device D.

```
DeviceD(config)# ip multicast-routing
DeviceD(config)# interface gigabitEthernet 0/6
DeviceD(config-if-GigabitEthernet 0/6)# ip pim sparse-mode
DeviceD(config-if-GigabitEthernet 0/6)# exit
DeviceD(config)# interface gigabitEthernet 0/7
DeviceD(config-if-GigabitEthernet 0/7)# ip pim sparse-mode
DeviceD(config-if-GigabitEthernet 0/7)# exit
```

Enable the multicast, PIM-SM, and IGMP functions on device E.

```
DeviceE(config)# ip multicast-routing
DeviceE(config)# interface gigabitEthernet 0/6
DeviceE(config-if-GigabitEthernet 0/6)# ip pim sparse-mode
DeviceE(config-if-GigabitEthernet 0/6)# exit
DeviceE(config)# interface gigabitEthernet 0/7
DeviceE(config-if-GigabitEthernet 0/7)# ip pim sparse-mode
DeviceE(config-if-GigabitEthernet 0/7)# exit
```

(3) Configure RPs.

Note

There are two methods to configure RPs: dynamic RPs and static RPs. You can configure either or both types of RPs. If static and dynamic RPs are available at the same time, the dynamic RPs are preferred by default.

Configure dynamic RPs. One or multiple multicast devices in the PIM-SM domain must be configured as C-RPs and C-BSRs. In this example, device B and device C are configured as C-RP and C-BSR. The address range of the served groups of the RP, as well as the interfaces of the C-RP and C-BSR are configured on device B and device C. The loopback interface is configured as the interface of the C-RP and C-BSR.

Configure C-RP and C-BSR and address range of the served groups of the RP on device B.

```
DeviceB(config)# ip pim bsr-candidate loopback 49
DeviceB(config)# ip access-list standard 49
DeviceB(config-std-nacl)# permit 224.0.0.0 0.255.255.255
DeviceB(config)# ip pim rp-candidate loopback 49 group-list 49
```

Configure C-RP and C-BSR and address range of the served groups of the RP on device C.

```
DeviceC(config)# ip pim bsr-candidate loopback 50
DeviceC(config)# ip access-list standard 50
DeviceC(config-std-nacl)# permit 225.0.0.0 0.255.255.255
DeviceC(config-std-nacl)# exit
DeviceC(config)# ip pim rp-candidate loopback 50 group-list 50
```

Configure static RPs. The addresses of static RPs must be specified on all multicast devices.

Configure a static RP on device A.

```
DeviceA(config)# ip pim rp-address 50.50.50.50
```

Configure a static RP on device B.

```
DeviceB(config)# ip pim rp-address 50.50.50.50
```

Configure a static RP on device C.

```
DeviceC(config)# ip pim rp-address 50.50.50.50
```

Configure a static RP on device D.

```
DeviceD(config)# ip pim rp-address 50.50.50.50
```

Configure a static RP on device E.

```
DeviceE(config)# ip pim rp-address 50.50.50.50
```

(4) Configure a BSR border on the device A interface connected to the Internet.

```
DeviceA(config-if-GigabitEthernet 0/1)# ip pim bsr-border
```

5. Verification

(1) Run the **show ip pim sparse-mode interface** command to display the PIM-SM running information on the interfaces.

The PIM-SM running information on the interface of device A is as follows:

```
DeviceA> enable
```

```
DeviceA#show ip pim sparse-mode interface
Address        Interface                          VIFindex Ver/Mode Nbr-Count
DR-Prior  DR
10.100.1.1     GigabitEthernet 0/21                 1       v2/S   0        1
10.100.1.1
10.100.3.2     GigabitEthernet 0/23                 2       v2/S   1        1
10.100.3.2
10.100.2.1     GigabitEthernet 0/24                 3       v2/S   0        1
10.100.2.1
DeviceA#
```

The PIM-SM running information on the interface of device B is as follows:

```
DeviceB> enable
DeviceB# show ip pim sparse-mode interface
Address        Interface                          VIFindex Ver/Mode Nbr-Count
DR-Prior  DR
10.100.8.1     GigabitEthernet 0/30                 1       v2/S   0        1
10.100.8.1
10.100.2.2     GigabitEthernet 0/31                 4       v2/S   1        1
10.100.2.2
10.100.5.2     GigabitEthernet 0/32                 2       v2/S   1        1
10.100.5.2
49.49.49.49    Loopback 49                         3       v2/S   0        1
49.49.49.49
DeviceB#
```

The PIM-SM running information on the interface of device C is as follows:

```
DeviceC> enable
DeviceC# show ip pim sparse-mode interface
Address        Interface                          VIFindex Ver/Mode Nbr-Count
DR-Prior  DR
10.100.6.1     GigabitEthernet 0/19                 1       v2/S   1        1
10.100.6.2
10.100.5.1     GigabitEthernet 0/20                 2       v2/S   1        1
10.100.5.2
10.100.3.1     GigabitEthernet 0/21                 3       v2/S   1        1
10.100.3.2
10.100.4.1     GigabitEthernet 0/22                 4       v2/S   1        1
10.100.4.2
50.50.50.50    Loopback 50                         5       v2/S   0        1
50.50.50.50
DeviceC#
```

The PIM-SM running information on the interface of device D is as follows:

```
DeviceD> enable
DeviceD# show ip pim sparse-mode interface
Address        Interface                          VIFindex Ver/Mode Nbr-Count
DR-Prior  DR
```

```
10.100.7.1     GigabitEthernet 0/6                  1        v2/S    0        1
10.100.7.1
10.100.6.2     GigabitEthernet 0/7                  2        v2/S    1        1
10.100.6.2
DeviceD#
```

The PIM-SM running information on the interface of device E is as follows:

```
DeviceE> enable
DeviceE# show ip pim sparse-mode interface
Address        Interface                          VIFindex Ver/Mode Nbr-Count
DR-Prior  DR
10.100.9.1     GigabitEthernet 0/6                  1        v2/S    0        1
10.100.9.1
10.100.4.2     GigabitEthernet 0/7                  2        v2/S    1        1
10.100.4.2
DeviceE#
```

(2) Run the **show ip pim sparse-mode bsr-router** command to display the election information of the BSRs.

The election information on device A is as follows:

```
DeviceA> enable
DeviceA# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
  BSR address: 50.50.50.50
  Uptime:     00:48:33, BSR Priority: 64, Hash mask length: 10
  Expires:    00:01:32
  Role: Non-candidate BSR   Priority: 0, Hash mask length: 10
  State: Accept Preferred
DeviceA#
```

The election information on device B is as follows:

```
DeviceB> enable
DeviceB# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
  BSR address: 50.50.50.50
  Uptime:     00:49:26, BSR Priority: 64, Hash mask length: 10
  Expires:    00:01:39
  Role: Candidate BSR   Priority: 64, Hash mask length: 10
  State: Candidate BSR

  Candidate RP: 49.49.49.49(Loopback 49)
    Advertisement interval 60 seconds
    Next Cand_RP_advertisement in 00:00:19
DeviceB#
```

The election information on device C is as follows:

```
DeviceC> enable
DeviceC# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
```

```
This system is the Bootstrap Router (BSR)
  BSR address: 50.50.50.50
  Uptime:     00:51:04, BSR Priority: 64, Hash mask length: 10
  Next bootstrap message in 00:00:56
  Role: Candidate BSR   Priority: 64, Hash mask length: 10
  State: Elected BSR
DeviceC#
```

The election information on device D is as follows:

```
DeviceD> enable
DeviceD# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
  BSR address: 50.50.50.50
  Uptime:     00:51:38, BSR Priority: 64, Hash mask length: 10
  Expires:    00:01:28
  Role: Non-candidate BSR   Priority: 0, Hash mask length: 10
  State: Accept Preferred
DeviceD#
```

The election information on device E is as follows:

```
DeviceE> enable
DeviceE# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
  BSR address: 50.50.50.50
  Uptime:     00:52:24, BSR Priority: 64, Hash mask length: 10
  Expires:    00:01:42
  Role: Non-candidate BSR   Priority: 0, Hash mask length: 10
  State: Accept Preferred
DeviceE#
```

(3) Run the **show ip pim sparse-mode rp mapping** command to display the RP information on the multicast devices.

The RP information on device A is as follows:

```
DeviceA> enable
DeviceA# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/8
  RP: 49.49.49.49(Not self)
    Info source: 50.50.50.50, via bootstrap, priority 192
        Uptime: 00:55:25, expires: 00:01:52
Group(s): 225.0.0.0/8
  RP: 50.50.50.50(Not self)
    Info source: 50.50.50.50, via bootstrap, priority 192
        Uptime: 00:00:48, expires: 00:01:52
Group(s): 224.0.0.0/4, Static
    RP: 50.50.50.50(Not self) , Static
        Uptime: 00:50:13
```

```
DeviceA#
```

The RP information on device B is as follows:

```
DeviceB> enable
DeviceB# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/8
  RP: 49.49.49.49(Self)
    Info source: 50.50.50.50, via bootstrap, priority 192
        Uptime: 00:56:12, expires: 00:02:05
Group(s): 225.0.0.0/8
  RP: 50.50.50.50(Not self)
    Info source: 50.50.50.50, via bootstrap, priority 192
        Uptime: 00:01:35, expires: 00:02:05
Group(s): 224.0.0.0/4, Static
    RP: 50.50.50.50(Not self) , Static
        Uptime: 00:49:36
DeviceB#
```

The RP information on device C is as follows:

```
DeviceC> enable
DeviceC# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/8
  RP: 49.49.49.49(Not self)
    Info source: 49.49.49.49, via bootstrap, priority 192
        Uptime: 00:56:17, expires: 00:02:13
Group(s): 225.0.0.0/8
  RP: 50.50.50.50(Self)
    Info source: 50.50.50.50, via bootstrap, priority 192
        Uptime: 00:01:40, expires: 00:01:50
Group(s): 224.0.0.0/4, Static
    RP: 50.50.50.50(Self) , Static
        Uptime: 00:49:39
DeviceC#
```

The RP information on device D is as follows:

```
DeviceD> enable
DeviceD# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/8
  RP: 49.49.49.49(Not self)
    Info source: 50.50.50.50, via bootstrap, priority 192
        Uptime: 00:56:22, expires: 00:01:55
Group(s): 225.0.0.0/8
  RP: 50.50.50.50(Not self)
    Info source: 50.50.50.50, via bootstrap, priority 192
```

```
        Uptime: 00:01:45, expires: 00:01:55
Group(s): 224.0.0.0/4, Static
    RP: 50.50.50.50(Not self) , Static
        Uptime: 00:49:40
DeviceD#
```

The RP information on device E is as follows:

```
DeviceE> enable
DeviceE# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/8
  RP: 49.49.49.49(Not self)
    Info source: 50.50.50.50, via bootstrap, priority 192
        Uptime: 00:56:27, expires: 00:01:50
Group(s): 225.0.0.0/8
  RP: 50.50.50.50(Not self)
    Info source: 50.50.50.50, via bootstrap, priority 192
        Uptime: 00:01:50, expires: 00:01:50
Group(s): 224.0.0.0/4, Static
    RP: 50.50.50.50(Not self) , Static
        Uptime: 00:49:43
DeviceE#
```

(4) Run the **show ip pim sparse-mode mroute** command to display the multicast routing tables of PIM-SM. The multicast source (10.100.1.2/24) sends traffic to the multicast groups (225.0.0.1/24) and (224.0.1.1/24). Host A joins the multicast group (225.0.0.1), and host B joins the multicast group (224.0.1.1).

The routing table information on device A is as follows:

```
DeviceA> enable
DeviceA# show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 2
(S,G,rpt) Entries: 2
FCR Entries: 0
REG Entries: 2

(10.100.1.2, 224.0.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 53 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
```

```
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Joined
0 . .
j . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
```

```
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

(10.100.1.2, 224.0.1.1, rpt)
RP: 50.50.50.50
RPF nbr: 10.100.3.1
RPF idx: GigabitEthernet 0/23
Upstream State: RPT NOT JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
Pruned
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

(10.100.1.2, 225.0.0.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 100 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Joined
0 . .
j . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

(10.100.1.2, 225.0.0.1, rpt)
RP: 50.50.50.50
RPF nbr: 10.100.3.1
RPF idx: GigabitEthernet 0/23
Upstream State: RPT NOT JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Pruned
```

```
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceA#
```

The routing table information on device B is as follows (only key information is displayed):

```
DeviceB> enable
DeviceB# show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 1
REG Entries: 0
```

```
(*, 225.0.0.1)
RP: 50.50.50.50
RPF nbr: 10.100.5.1
RPF idx: GigabitEthernet 0/32
Upstream State: JOINED
jt_timer expires in 52 seconds
FCR:
Source: 10.100.1.2
KAT timer running, 166 seconds remaining
 Packet count 1

DeviceB#
```

The routing table information on device C is as follows (only key information is displayed):

```
DeviceC> enable
DeviceC# show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 2
(S,G) Entries: 2
(S,G,rpt) Entries: 2
FCR Entries: 0
REG Entries: 0

(*, 224.0.1.1)
RP: 50.50.50.50
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
FCR:

(10.100.1.2, 224.0.1.1)
RPF nbr: 10.100.3.2
RPF idx: GigabitEthernet 0/21
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 15 seconds
kat expires in 203 seconds

(10.100.1.2, 224.0.1.1, rpt)
RP: 50.50.50.50
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: PRUNED
```

```
(*, 225.0.0.1)
RP: 50.50.50.50
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
FCR:

(10.100.1.2, 225.0.0.1)
RPF nbr: 10.100.3.2
RPF idx: GigabitEthernet 0/21
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 23 seconds
kat expires in 176 seconds

(10.100.1.2, 225.0.0.1, rpt)
RP: 50.50.50.50
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: PRUNED

DeviceC#
```

The routing table information on device E is as follows (only key information is displayed):

```
DeviceE> enable
DeviceE# show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 1
REG Entries: 0

(*, 224.0.1.1)
RP: 50.50.50.50
RPF nbr: 10.100.4.1
RPF idx: GigabitEthernet 0/7
Upstream State: JOINED
jt_timer expires in 34 seconds
FCR:
Source: 10.100.1.2
KAT timer running, 156 seconds remaining
 Packet count 1

DeviceE#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.100.1.1 255.255.255.0
 ip pim sparse-mode
 ip pim bsr-border
!
interface GigabitEthernet 0/21
 no switchport
 ip address 10.100.1.1 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/23
 no switchport
 ip address 10.100.3.2 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/24
 no switchport
 ip address 10.100.2.1 255.255.255.0
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.1.0 0.0.0.255 area 0
 network 10.100.2.0 0.0.0.255 area 0
 network 10.100.3.0 0.0.0.255 area 0
 network 10.100.10.0 0.0.0.255 area 0
!
ip pim rp-address 50.50.50.50
!
```

- Device B configuration file

```
hostname DeviceB
!
ip access-list standard 49
 20 permit 224.0.0.0 0.255.255.255
!
ip multicast-routing
!
interface GigabitEthernet 0/30
```

```
 no switchport
 ip address 10.100.8.1 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/31
 no switchport
 ip address 10.100.2.2 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/32
 no switchport
 ip address 10.100.5.2 255.255.255.0
 ip pim sparse-mode
!
interface Loopback 49
 ip address 49.49.49.49 255.255.255.255
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.2.0 0.0.0.255 area 0
 network 10.100.5.0 0.0.0.255 area 0
 network 10.100.8.0 0.0.0.255 area 0
 network 49.49.49.49 0.0.0.0 area 0
!
ip pim rp-address 50.50.50.50
ip pim bsr-candidate Loopback 49
ip pim rp-candidate Loopback 49 group-list 49
!
```

- Device C configuration file

```
hostname DeviceC
!
ip access-list standard 50
 10 permit 225.0.0.0 0.255.255.255
!
ip multicast-routing
!
interface GigabitEthernet 0/19
 no switchport
 ip address 10.100.6.1 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/20
 no switchport
 ip address 10.100.5.1 255.255.255.0
 ip pim sparse-mode
```

```
!
interface GigabitEthernet 0/21
 no switchport
 ip address 10.100.3.1 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/22
 no switchport
 ip address 10.100.4.1 255.255.255.0
 ip pim sparse-mode
!
interface Loopback 50
 ip address 50.50.50.50 255.255.255.255
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.3.0 0.0.0.255 area 0
 network 10.100.4.0 0.0.0.255 area 0
 network 10.100.5.0 0.0.0.255 area 0
 network 10.100.6.0 0.0.0.255 area 0
 network 50.50.50.50 0.0.0.0 area 0
!
ip pim rp-address 50.50.50.50
ip pim bsr-candidate Loopback 50
ip pim rp-candidate Loopback 50 group-list 50
!
```

- Device D configuration file

```
hostname DeviceD
!
ip multicast-routing
!
interface GigabitEthernet 0/6
 no switchport
 ip address 10.100.7.1 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/7
 no switchport
 ip address 10.100.6.2 255.255.255.0
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.6.0 0.0.0.255 area 0
 network 10.100.7.0 0.0.0.255 area 0
```

```
!
ip pim rp-address 50.50.50.50
!
```

- Device E configuration file

```
hostname DeviceE
!
ip multicast-routing
!
interface GigabitEthernet 0/6
 no switchport
 ip address 10.100.9.1 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/7
 no switchport
 ip address 10.100.4.2 255.255.255.0
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.4.0 0.0.0.255 area 0
 network 10.100.9.0 0.0.0.255 area 0
!
ip pim rp-address 50.50.50.50
!
```

7. Common Errors

- The multicast routing function is not enabled on multicast devices.
- The multicast function is not enabled on any interface.
- No BSR border is configured between PIM-SM domains.
- No RP is configured.
- No static RP is configured on a multicast device, or the configured static RP on this multicast device is not consistent with the configuration on other multicast devices.
- C-RPs are configured, but no C-BSR is configured.
- Static RP, C-RP or C-BSR is unreachable via unicast routes.

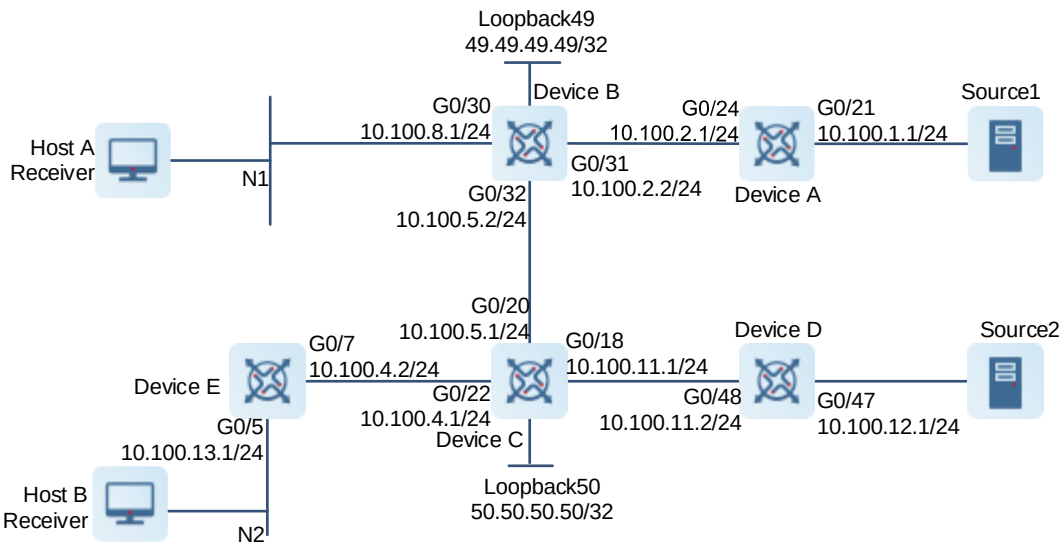
1.14.2 Configuring Basic Functions of PIM-SM in the SSM Model

1. Requirements

As shown in Figure 1-6, the PIM-SM protocol is enabled on multicast devices to provide SSM services for hosts in N1 and N2 so that the hosts can receive multicast data from specified multicast sources to the multicast group that the hosts join, for example, video-on-demand.

2. Topology

Figure 1-6 PIM-SM Multicast Network Topology in the SSM Model



3. Notes

- Configure IP addresses and unicast routing protocols for multicast devices. The PIM routing protocol in a multicast domain depends on unicast routing protocols. Normal communication of unicast routing lays a foundation of multicast routing. Ensure that each PIM node is reachable via unicast routes.
- Enable the multicast function on all multicast devices. Enabling the multicast function is a prerequisite of PIM-SM configuration.
- Enable the basic functions of PIM-SM on all interfaces of the multicast devices. The other functions of PIM-SM can be enabled only after the basic functions of PIM-SM are enabled.
- Enable the IGMP function on the interface connected to hosts and set the IGMP version to v3 so that the hosts can join or leave a multicast group by sending IGMP messages based on the specified source. The multicast devices acting as leaf nodes maintain group membership based on the IGMP protocol.
- Configure the same address range of SSM on all multicast devices. The SSM services provided by the multicast devices in the PIM-SM domain are dedicated to specified groups, which realizes multicast controllability.

4. Procedure

(1) Configure IP addresses and enable unicast routing protocols on interfaces of different devices.

Configure IP addresses and enable unicast routing protocols on interfaces of device A.

```
DeviceA> enable
DeviceA# config terminal
DeviceA(config)# interface GigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# no switchport
DeviceA(config-if-GigabitEthernet 0/21)# ip address 10.100.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/21)# exit
```

```
DeviceA(config)# interface GigabitEthernet 0/24
DeviceA(config-if-GigabitEthernet 0/24)# no switchport
DeviceA(config-if-GigabitEthernet 0/24)# ip address 10.100.2.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/24)# exit
DeviceA(config)# router ospf 49
DeviceA(config-router)# network 10.100.1.0 0.0.0.255 area 0
DeviceA(config-router)# network 10.100.2.0 0.0.0.255 area 0
DeviceA(config-router)# exit
```

Configure IP addresses and enable unicast routing protocols on interfaces of device B.

```
DeviceB> enable
DeviceB# config terminal
DeviceB(config)# interface GigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# no switchport
DeviceB(config-if-GigabitEthernet 0/30)# ip address 10.100.8.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface GigabitEthernet 0/31
DeviceB(config-if-GigabitEthernet 0/31)# no switchport
DeviceB(config-if-GigabitEthernet 0/31)# ip address 10.100.2.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/31)# exit
DeviceB(config)#interface GigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# no switchport
DeviceB(config-if-GigabitEthernet 0/32)# ip address 10.100.5.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface Loopback 49
DeviceB(config-if-Loopback 49)# ip address 49.49.49.49 255.255.255.255
DeviceB(config-if-Loopback 49)# exit
DeviceB(config)# router ospf 49
DeviceB(config-router)# network 10.100.2.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.5.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.8.0 0.0.0.255 area 0
DeviceB(config-router)# network 49.49.49.49 0.0.0.0 area 0
DeviceB(config-router)# exit
```

Configure IP addresses and enable unicast routing protocols on interfaces of device C.

```
DeviceC> enable
DeviceC# config terminal
DeviceC(config)# interface GigabitEthernet 0/18
DeviceC(config-if-GigabitEthernet 0/18)# no switchport
DeviceC(config-if-GigabitEthernet 0/18)# ip address 10.100.11.1 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/18)# exit
DeviceC(config)#interface GigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# no switchport
DeviceC(config-if-GigabitEthernet 0/20)# ip address 10.100.5.1 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface GigabitEthernet 0/22
DeviceC(config-if-GigabitEthernet 0/22)# no switchport
```

```
DeviceC(config-if-GigabitEthernet 0/22)# ip address 10.100.4.1 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/22)# exit
DeviceC(config)# interface Loopback 50
DeviceC(config-if-Loopback 50)# ip address 50.50.50.50 255.255.255.255
DeviceC(config-if-Loopback 50)# exit
DeviceC(config)# router ospf 49
DeviceC(config-router)# network 10.100.4.0 0.0.0.255 area 0
DeviceC(config-router)# network 10.100.5.0 0.0.0.255 area 0
DeviceC(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceC(config-router)# network 50.50.50.50 0.0.0.0 area 0
DeviceC(config-router)# exit
```

Configure IP addresses and enable unicast routing protocols on interfaces of device D.

```
DeviceD> enable
DeviceD# config terminal
DeviceD(config)# interface GigabitEthernet 0/47
DeviceD(config-if-GigabitEthernet 0/47)# no switchport
DeviceD(config-if-GigabitEthernet 0/47)# ip address 10.100.12.1 255.255.255.0
DeviceD(config-if-GigabitEthernet 0/47)# exit
DeviceD(config)# interface GigabitEthernet 0/48
DeviceD(config-if-GigabitEthernet 0/48)# no switchport
DeviceD(config-if-GigabitEthernet 0/48)# ip address 10.100.11.2 255.255.255.0
DeviceD(config-if-GigabitEthernet 0/48)# exit
DeviceD(config)# router ospf 49
DeviceD(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceD(config-router)# network 10.100.12.0 0.0.0.255 area 0
DeviceD(config-router)# exit
DeviceD(config)# router ospf 49
DeviceD(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceD(config-router)# network 10.100.12.0 0.0.0.255 area 0
DeviceD(config-router)# exit
```

Configure IP addresses and enable unicast routing protocols on interfaces of device E.

```
DeviceE> enable
DeviceE# config terminal
DeviceE(config)# interface GigabitEthernet 0/5
DeviceE(config-if-GigabitEthernet 0/5)# no switchport
DeviceE(config-if-GigabitEthernet 0/5)# ip address 10.100.13.1 255.255.255.0
DeviceE(config-if-GigabitEthernet 0/5)# exit
DeviceE(config)# interface GigabitEthernet 0/7
DeviceE(config-if-GigabitEthernet 0/7)# no switchport
DeviceE(config-if-GigabitEthernet 0/7)# ip address 10.100.4.2 255.255.255.0
DeviceE(config-if-GigabitEthernet 0/7)# exit
DeviceE(config)# router ospf 49
DeviceE(config-router)# network 10.100.4.0 0.0.0.255 area 0
DeviceE(config-router)# network 10.100.13.0 0.0.0.255 area 0
DeviceE(config-router)# exit
```

(2) Enable the multicast and PIM-SM functions on all multicast devices, and enable the IGMP function on all multicast devices connected to hosts.

Enable the multicast and PIM-SM functions on device A.

```
DeviceA(config)# ip multicast-routing
DeviceA(config)# interface GigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/21)# exit
DeviceA(config)# interface GigabitEthernet 0/24
DeviceA(config-if-GigabitEthernet 0/24)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/24)# exit
```

Enable the multicast, PIM-SM, and IGMP functions on device B, and set the IGMP version to v3.

```
DeviceB(config)# ip multicast-routing
DeviceB(config)# interface GigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# ip pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/30)# ip igmp version 3
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface GigabitEthernet 0/31
DeviceB(config-if-GigabitEthernet 0/31)# ip pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/31)# exit
DeviceB(config)# interface GigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# ip pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface Loopback 49
DeviceB(config-if-Loopback 49)# ip pim sparse-mode
DeviceB(config-if-Loopback 49)# exit
```

Enable the multicast and PIM-SM functions on device C.

```
DeviceC(config)# ip multicast-routing
DeviceC(config)# interface GigabitEthernet 0/18
DeviceC(config-if-GigabitEthernet 0/18)# ip pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/18)# exit
DeviceC(config)# interface GigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# ip pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface GigabitEthernet 0/22
DeviceC(config-if-GigabitEthernet 0/22)# ip pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/22)# exit
DeviceC(config)#interface Loopback 50
DeviceC(config-if-Loopback 50)# ip pim sparse-mode
DeviceC(config-if-Loopback 50)# exit
```

Enable the multicast and PIM-SM functions on device D.

```
DeviceD(config)# ip multicast-routing
DeviceD(config)# interface GigabitEthernet 0/47
DeviceD(config-if-GigabitEthernet 0/47)# ip pim sparse-mode
DeviceD(config-if-GigabitEthernet 0/47)# exit
```

```
DeviceD(config)# interface GigabitEthernet 0/48
DeviceD(config-if-GigabitEthernet 0/48)# ip pim sparse-mode
DeviceD(config-if-GigabitEthernet 0/48)# exit
```

Enable the multicast, PIM-SM, and IGMP functions on device E, and set the IGMP version to v3.

```
DeviceE(config)# ip multicast-routing
DeviceE(config)# interface GigabitEthernet 0/5
DeviceE(config-if-GigabitEthernet 0/5)# ip pim sparse-mode
DeviceE(config-if-GigabitEthernet 0/5)# ip igmp version 3
DeviceE(config-if-GigabitEthernet 0/5)# exit
DeviceE(config)# interface GigabitEthernet 0/7
DeviceE(config-if-GigabitEthernet 0/7)# ip pim sparse-mode
DeviceE(config-if-GigabitEthernet 0/7)# exit
```

(3) Enable the SSM function and configure an address range of multicast groups on all multicast devices.

Set the address range of an SSM multicast group to 232.1.1.0/24 on device A.

```
DeviceA(config)# ip access-list standard 59
DeviceA(config-std-nacl)#permit 232.1.1.0 0.0.0.255
DeviceA(config-std-nacl)#exit
DeviceA(config)# ip pim ssm range 59
```

Set the address range of an SSM multicast group to 232.1.1.0/24 on device B.

```
DeviceB(config)# ip access-list standard 59
DeviceB(config-std-nacl)#permit 232.1.1.0 0.0.0.255
DeviceB(config-std-nacl)#exit
DeviceB(config)# ip pim ssm range 59
```

Set the address range of an SSM multicast group to 232.1.1.0/24 on device C.

```
DeviceC(config)# ip access-list standard 59
DeviceC(config-std-nacl)#permit 232.1.1.0 0.0.0.255
DeviceC(config-std-nacl)#exit
DeviceC(config)# ip pim ssm range 59
```

Set the address range of an SSM multicast group to 232.1.1.0/24 on device D.

```
DeviceD(config)# ip access-list standard 59
DeviceD(config-std-nacl)#permit 232.1.1.0 0.0.0.255
DeviceD(config-std-nacl)#exit
DeviceD(config)# ip pim ssm range 59
```

Set the address range of an SSM multicast group to 232.1.1.0/24 on device E.

```
DeviceE(config)# ip access-list standard 59
DeviceE(config-std-nacl)#permit 232.1.1.0 0.0.0.255
DeviceE(config-std-nacl)#exit
DeviceE(config)# ip pim ssm range 59
```

5. Verification

(1) Run the **show ip pim sparse-mode interface** command to display PIM-SM running information on the interfaces. The PIM-SM running information on the interfaces of device A is as follows. The PIM-SM running information on the interfaces of devices B, C, D, and E is the same.

```
DeviceA> enable
DeviceA# show ip pim sparse-mode interface
Address        Interface                          VIFindex Ver/Mode Nbr-Count
DR-Prior  DR
10.100.1.1     GigabitEthernet 0/21                  3        v2/S    0        1
10.100.1.1
10.100.2.1     GigabitEthernet 0/24                  1        v2/S    0        1
10.100.2.1
DeviceA#
```

(2) Run the **show ip pim sparse-mode mroute** command to display the multicast routing tables of PIM-SM. Host A needs to receive packets sent from source 1 (10.100.1.2/24) and source 2 (10.100.12.2/24) to the multicast group (232.1.1.10/24). Host B needs to receive packets sent from source 1 (10.100.1.2/24) to the multicast group (232.1.1.10/24). The information output is as follows:

The routing table information on device A is as follows:

```
DeviceA> enable
DeviceA# show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 0
FCR Entries: 0
REG Entries: 0

(10.100.1.2, 232.1.1.10)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 133 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
```

```
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Joined
0 . . . .
j . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceA#
```

The routing table information on device B is as follows:

```
DeviceB> enable
DeviceB# show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 2
(S,G,rpt) Entries: 0
FCR Entries: 0
REG Entries: 0

(10.100.1.2, 232.1.1.10)
RPF nbr: 10.100.2.1
RPF idx: GigabitEthernet 0/31
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 40 seconds
kat expires in 190 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . .
i . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Joined
0 . .
j . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . o .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

(10.100.12.2, 232.1.1.10)
RPF nbr: 10.100.5.1
RPF idx: GigabitEthernet 0/32
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 40 seconds
kat expires in 125 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . .
i . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceB#
```

The routing table information on device C is as follows:

```
DeviceC> enable
DeviceC# show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 2
(S,G,rpt) Entries: 0
FCR Entries: 0
REG Entries: 0

(10.100.1.2, 232.1.1.10)
RPF nbr: 10.100.5.2
RPF idx: GigabitEthernet 0/20
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 12 seconds
kat expires in 72 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
0  .  .  .  .  .
j  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
```

```
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

(10.100.12.2, 232.1.1.10)
```

```
RPF nbr: 10.100.11.2
RPF idx: GigabitEthernet 0/18
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 8 seconds
kat expires in 98 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
0  .  .  .  .
j  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
```

```
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceC#
```

The routing table information on device D is as follows:

```
DeviceD> enable
DeviceD# show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 0
FCR Entries: 0
REG Entries: 0

(10.100.12.2, 232.1.1.10)
```

```
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 62 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
0  .  .
j  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
```

```
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceD#
```

The routing table information on device E is as follows:

```
DeviceE> enable
DeviceE# show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 0
FCR Entries: 0
REG Entries: 0

(10.100.1.2, 232.1.1.10)
RPF nbr: 10.100.4.1
RPF idx: GigabitEthernet 0/7
```

```
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 39 seconds
kat expires in 189 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .
i  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
```

```
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceE#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip access-list standard 59
 10 permit 232.1.1.0 0.0.0.255
!
ip multicast-routing
!
interface GigabitEthernet 0/21
 no switchport
 ip address 10.100.1.1 255.255.255.0
ip pim sparse-mode
```

```
!
interface GigabitEthernet 0/24
 no switchport
 ip address 10.100.2.1 255.255.255.0
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.1.0 0.0.0.255 area 0
 network 10.100.2.0 0.0.0.255 area 0
!
ip pim ssm range 59
!
```

- Device B configuration file

```
hostname DeviceB
!
ip access-list standard 59
 10 permit 232.1.1.0 0.0.0.255
!
ip multicast-routing
!
interface GigabitEthernet 0/30
 no switchport
 ip address 10.100.8.1 255.255.255.0
 ip igmp version 3
 ip pim sparse-mode
!
interface GigabitEthernet 0/31
 no switchport
 ip address 10.100.2.2 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/32
 no switchport
 ip address 10.100.5.2 255.255.255.0
 ip pim sparse-mode
!
interface Loopback 49
 ip address 49.49.49.49 255.255.255.255
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.2.0 0.0.0.255 area 0
 network 10.100.5.0 0.0.0.255 area 0
 network 10.100.8.0 0.0.0.255 area 0
```

```
 network 49.49.49.49 0.0.0.0 area 0
!
ip pim ssm range 59
!
```

- Device C configuration file

```
hostname DeviceC
!
ip access-list standard 59
 10 permit 232.1.1.0 0.0.0.255
!
ip multicast-routing
!
interface GigabitEthernet 0/18
 no switchport
 ip address 10.100.11.1 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/20
 no switchport
 ip address 10.100.5.1 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/22
 no switchport
 ip address 10.100.4.1 255.255.255.0
 ip pim sparse-mode
!
interface Loopback 50
 ip address 50.50.50.50 255.255.255.255
ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.4.0 0.0.0.255 area 0
 network 10.100.5.0 0.0.0.255 area 0
 network 10.100.11.0 0.0.0.255 area 0
 network 50.50.50.50 0.0.0.0 area 0
!
ip pim ssm range 59
!
```

- Device D configuration file

```
hostname DeviceD
!
ip access-list standard 59
 10 permit 232.1.1.0 0.0.0.255
```

```
!
ip multicast-routing
!
interface GigabitEthernet 0/47
 no switchport
 ip address 10.100.12.1 255.255.255.0
ip pim sparse-mode
!
interface GigabitEthernet 0/48
 no switchport
 ip address 10.100.11.2 255.255.255.0
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.12.0 0.0.0.255 area 0
!
ip pim ssm range 59
!
```

- Device E configuration file

```
hostname DeviceE
!
ip access-list standard 59
 10 permit 232.1.1.0 0.0.0.255
!
ip multicast-routing
!
interface GigabitEthernet 0/5
 no switchport
 ip address 10.100.13.1 255.255.255.0
 ip igmp version 3
 ip pim sparse-mode
!
interface GigabitEthernet 0/7
 no switchport
 ip address 10.100.4.2 255.255.255.0
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.4.0 0.0.0.255 area 0
 network 10.100.13.0 0.0.0.255 area 0
!
ip pim ssm range 59
!
```

7. Common Errors

- An IPv4 unicast route is incorrectly configured.
- IPv4 multicast routing is not enabled on a multicast device.
- The SSM function is not enabled on a multicast device, or the SSM group address range on this multicast device is not consistent with the configuration on other multicast devices.
- The PIM-SM function is not enabled on an interface, for example, the gateway interface connecting to hosts or a multicast source.
- IGMPv3 is not enabled on an interface connected to hosts.

Contents

1 Configuring PIM-DM....1
1.1 Introduction....1
1.1.1 Overview....1
1.1.2 PIM-DM Network Deployment....1
1.1.3 Principles....1
1.1.4 PIM-DM and MIB....4
1.1.5 Protocols and Standards....4
1.2 Restrictions and Guidelines....4
1.3 Configuration Task Summary....4
1.4 Configuring Basic Functions of PIM-DM....4
1.4.1 Overview....4
1.4.2 Procedure....4
1.5 Configuring PIM-DM Passive Mode....5
1.5.1 Overview....5
1.5.2 Procedure....5
1.6 Configuring PIM Neighbors....6
1.6.1 Overview....6
1.6.2 Procedure....6
1.7 Configuring PIM State Refresh....6
1.7.1 Overview....6
1.7.2 Restrictions and Guidelines....7
1.7.3 Procedure....7

1.8 Enabling the PIM-BFD Function 7

1.8.1 Overview 7

1.8.2 Procedure 7

1.9 Enabling the MIB Function 8

1.9.1 Overview 8

1.9.2 Procedure 8

1.10 Monitoring 8

1 Configuring PIM-DM

1.1 Introduction

1.1.1 Overview

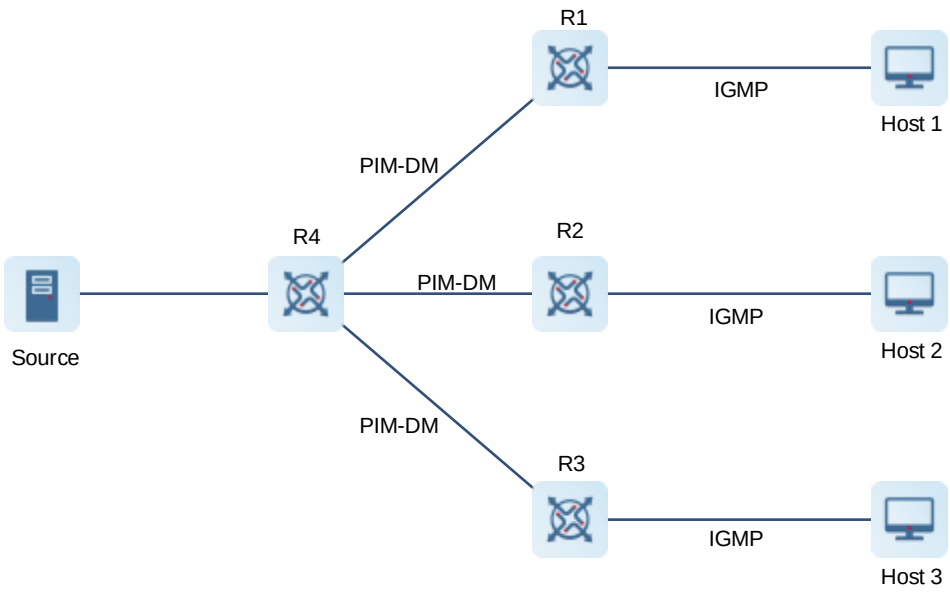
In multicast packet transmission, devices need to run multicast routing protocols to control multicast packet forwarding. A multicast network can be composed of multiple domains. The most typical multicast routing protocol is Protocol Independent Multicast (PIM). Based on implementation mechanism, PIM is categorized into Protocol Independent Multicast-Dense Mode (PIM-DM) and Protocol Independent Multicast-Sparse Mode (PIM-SM).

PIM-DM runs on multicast devices and is used to discover and maintain multicast routing information and determine a forwarding route of multicast packets.

Compared with PIM-SM, PIM-DM applies to small networks where multicast group members densely reside. Ideally, multicast group members on every path need to receive packets in the PIM network, and each forwarding node pushes and distributes the multicast packets in the entire network.

1.1.2 PIM-DM Network Deployment

Figure 1-1 PIM-DM Deployment Topology



As shown in Figure 1-1, when a multicast device is connected to other multicast devices, PIM must be deployed on this multicast device. Here, PIM-DM is deployed.

1.1.3 Principles

The basic principles of PIM-DM are as follows:

(1) Assume that all paths in a network have multicast group members and the multicast source sends multicast packets throughout the entire network.

(2) The entire path can be considered a tree with the source as the root node and group members as leaf nodes. This tree is the shortest path tree (SPT). Initially, some leaf nodes are not group members and they must be pruned to get a correct tree structure.

(3) If a new host joins the tree or an existing node leaves the tree, the tree structure must be readjusted. Multicast packets are forwarded on the paths of this tree, and the forwarding path is the shortest path from the source to the group members.

The working mechanisms of PIM-DM include neighbor creation, flooding, pruning, state refresh, graft, and assertion.

1. Neighbor Creation

Neighbors are the basis of PIM-DM. Neighbor relationships must be created between PIM routers before PIM control messages can be exchanged or multicast packets can be forwarded.

Neighbor creation is implemented based on the hello messages sent by the PIM interfaces and is composed of neighbor discovery, protocol parameter negotiation, and neighbor relationship maintenance.

- Discover neighbors

  A PIM interface periodically sends hello messages with the destination address being 224.0.0.13 (ff02::d for IPv6), source address being the IP address of the interface, and time to live (TTL) value being **1**. PIM routers in the same network segment receive the packets with the destination address 224.0.0.13 (ff02::d for IPv6). In this way, the PIM routers obtain neighbor information and create neighbor relationships.

  When a PIM interface is enabled or detects a new neighbor, a Triggered-Hello-Delay message is used to generate a random time. Within the time, the interface sends hello messages.

- Negotiate protocol parameters

  Protocol parameters are negotiated by hello messages. The key parameters are described as follows:

  - **DR_Priority**: The priority of a router for designated router (DR) election. The router with a higher priority is selected.
  - **Holdtime**: The neighbor is considered reachable within the hold time.
  - **Propagation Delay**: Duration between the time when a PIM device receives a prune packet and the time when the PIM device sends the prune packet to the upstream devices.
  - **Override-Interval**: The interval to override the prune.

- Maintain neighbor relationship

  A hello message is sent periodically between PIM routers. If a hello message is not received from a PIM neighbor within the hold time, the neighbor is considered unreachable and is deleted from the neighbor list. Any change of PIM neighbors will cause change of the multicast topology in the network. If an upstream or a downstream neighbor in a multicast distribution tree (MDT) is unreachable, multicast routes converge again and the MDT is reshaped.

2. Flooding

Multicast packets flooded to an entire network from a source is referred to flooding. Flooding enables all nodes in a network to receive these packets.

Multicast devices check reverse path forwarding (RPF) in the packets. If the checking fails, the packets are discarded. If the checking is passed and an outbound interface is detected, the multicast packets are forwarded through the outbound interface. This enables all node members in the network to receive these multicast packets.

3. Pruning

If no group member exists on a path branch, the path branch is pruned. This enables packets to be forwarded to paths with group members available.

(1) Multicast devices check RPF in the packets. If the checking is passed but no outbound interface exists, no group member exists on this path. A prune packet is sent to the upstream device.

(2) Upon receiving the prune packet, the upstream device marks the packet sending interface as pruned and sets a prune state timer.

(3) After all unnecessary paths are pruned, the remaining paths are necessary and they form an SPT.

- Prune override

After a PIM router sends a prune packet to the upstream device, the PIM router does not prune the downstream path immediately. If the downstream device has multicast requirements, it can send a prune override message to the PIM router to override the prune.

If the PIM router receives a prune override message from the downstream device in the prune-pending timer (PPT), the PIM router cancels pruning. PPT = Propagation delay + Override interval

4. State Refresh

A prune state timer is maintained on a device during pruning. When the timer times out, the device continues to forward packets. PIM-DM refreshes the timer state using a state refresh message (SRM) to avoid unnecessary prune state changes.

The multicast device nearest to the source periodically sends the SRM to the downstream devices. Upon receiving the SRM, the downstream devices add the local topology state information to the SRM by modifying some fields in the SRM, and continue to forward the SRM to downstream devices. Finally, the SRM arrives leaf devices and the states of all devices in the network get updated.

5. Graft

If a group member sends data to a group corresponding to a path being pruned, the path must be restored to the forwarding state. This is referred to as graft.

(1) When a group member sends data to a group corresponding to a path being pruned, the other devices on this path receive the join message and send a graft packet to the upstream device to apply for joining the SPT.

(2) Upon receiving the graft packet, the upstream device replies a Graft-Ack packet and starts to forward multicast packets to the downstream devices on this path.

(3) The downstream devices receive the Graft-Ack packet. If the downstream devices do not receive the Graft-Ack packet, they send the graft packet again and again until they receive the Graft-Ack packet.

6. Assertion

In a network segment where multiple PIM routers reside, the same multicast packet may be transmitted to the routers in the network segment multiple times. In this case, a special PIM router can be specified to forward multicast packets and avoid duplicate forwarding. This is referred to as assertion.

1.1.4 PIM-DM and MIB

Connected to other agents, the Simple Network Management Protocol (SNMP) manager uses information in the Management Information Base (MIB) to directly manage the PIM-DM function.

The MIB specifies variables (namely information that can be queried and set by the management process) maintained by network elements and directly manages the PIM-DM function.

1.1.5 Protocols and Standards

- RFC3973: Protocol Independent Multicast - Dense Mode (PIM-DM)
- RFC2715: Interoperability Rules for Multicast Routing Protocols

1.2 Restrictions and Guidelines

- If PIM-DM neighbor relationships between devices are created through links and downstream devices have no or few needs to receive multicast packets, the system performance is excessively consumed. In this scenario, PIM-SM is recommended for the environment deployment.
- Before PIM-DM is used, ensure that unicast routes are reachable in the network.

1.3 Configuration Task Summary

The PIM-DM configuration includes the following tasks:

(1) Configuring Basic Functions of PIM-DM

(2) (Optional) Configuring PIM-DM Passive Mode

(3) (Optional) Configuring PIM Neighbors

(4) (Optional) Configuring PIM State Refresh

(5) (Optional) Enabling the PIM-BFD Function

(6) (Optional) Enabling the MIB Function

1.4 Configuring Basic Functions of PIM-DM

1.4.1 Overview

A PIM network is created to provide IPv4 multicast services for sources and hosts in the network. Neighbor relationships must be created between PIM routers before PIM control messages can be exchanged or multicast packets can be forwarded.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IPv4 multicast routing.

ip multicast-routing

The multicast routing function is disabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Enable the PIM-DM function.

ip pim dense-mode

The PIM-DM function is disabled on an interface by default.

The function can be enabled on the interconnection interfaces of routers, and interfaces connecting to multicast sources and user hosts.

(6) (Optional) Enable the PIM-DM function on a super VLAN interface.

ip pim dense-mode subvlan [**all** | *subvlan-id*]

The PIM-DM function is disabled on a super VLAN interface by default.

In most scenarios, the PIM-DM protocol is disabled by default and not needed on a super VLAN interface. This interface does not send or receive PIM packets. To enable PIM-DM to run on the super VLAN interface, specify a sub VLAN or all sub VLANs to receive packets. Note that if all sub VLANs are specified to receive packets, the transmission performance may be reduced, causing neighbor flapping.

1.5 Configuring PIM-DM Passive Mode

1.5.1 Overview

In a PIM network, if you want an interface, for example, a stub network device interface connecting to hosts, to receive multicast packets without involving the PIM network topology construction, you can set the interface to the PIM-DM passive mode. After the PIM-SM passive mode is configured, the interface does not process PIM-DM packets.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the PIM-DM passive mode on an interface.

ip pim dense-mode passive

The PIM-DM passive mode is disabled on an interface by default.

1.6 Configuring PIM Neighbors

1.6.1 Overview

PIM devices support adjustment to protocol parameters in hello messages and neighbor filtering to improve network security.

1.6.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure PIM neighbors. The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Configure hello message sending interval.

  ip pim query-interval *query-interval*

  Hello messages are sent at an interval of **30** seconds by default.

  Every time when the hello message sending interval is updated, the hello message hold time value is automatically updated as 3.5 times the interval. If the product of the hello message sending interval and 3.5 is greater than 65,535, the hello message hold time value is updated as 65,535.

- Configure propagation delay of hello messages on an interface.

  ip pim propagation-delay *propagation-delay-time*

  The default propagation delay of hello messages on an interface is **500** ms.

- Configure prune override interval of hello messages.

  ip pim override-interval *override-interval*

  The default prune override interval of hello messages is **2500** ms.

- Configure PIM neighbor filtering.

  ip pim neighbor-filter { *acl-name* | *acl-number* }

  The neighbor filtering function is disabled on an interface by default.

  Only addresses that meet ACL filtering conditions can be used as PIM neighbors of the current interface. Otherwise, the addresses filtered out cannot be neighbors.

1.7 Configuring PIM State Refresh

1.7.1 Overview

PIM devices support enabling or disabling PIM state refresh and adjusting PIM SRM sending interval.

1.7.2 Restrictions and Guidelines

- If the state refresh function is disabled, SRMs are not processed or forwarded.
- Disabling the state refresh function may cause the converged PIM-DM MDT to re-converge, which leads to unnecessary bandwidth waste and multicast routing table flapping. Therefore, you are not advised to disable this function in general conditions.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the PIM-DM state refresh function. The following configuration tasks are optional. Select tasks for configuration according to actual condition.

- Disable the PIM-DM state refresh function on an interface.

  ip pim state-refresh disable

  The PIM-DM SRMs are processed and forwarded by default.

- Configure the PIM-DM SRM sending interval on an interface.

  ip pim state-refresh origination-interval *origination-interval*

  The PIM-DM SRMs are sent at an interval of **60** seconds by default.

1.8 Enabling the PIM-BFD Function

1.8.1 Overview

PIM-DM supports correlation with the bidirectional forwarding detection (BFD) function. After the PIM-BFD function is enabled on the interconnection interfaces of routers, the interfaces are used as BFD interfaces to quickly detect neighbor changes and specify a router to forward multicast packets in a specified network segment based on the assertion rule.

1.8.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the PIM-BFD function on an interface.

ip pim bfd

The PIM-BFD function is disabled on an interface by default.

1.9 Enabling the MIB Function

1.9.1 Overview

The MIB function allows PIM devices to manage PIM-DM using the elements in the MIB.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the MIB function to manage PIM-DM.

ip pim mib dense-mode

PIM-DM is not managed by the MIB function by default.

1.10 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear ip pim dense-mode track	Clears statistical information about PIM-DM protocol packets.
show ip pim dense-mode interface [*interface-type interface-number*] [**detail**]	Displays PIM-DM interface information.
show ip pim dense-mode neighbor [*interface-type interface-number*]	Displays the PIM-DM neighbor information.
show ip pim dense-mode nexthop	Displays the PIM-DM next hop information.
show ip pim dense-mode mroute [*group-or-source-address-1* [*group-or-source-address-2*]] [**summary**]	Displays information about the PIM-DM routing table.
show ip pim dense-mode track	Displays statistical information about PIM-DM protocol packets.

Contents

1 Configuring IGMP Snooping 1
1.1 Introduction 1
1.1.2 Principles 1
1.1.3 Port Types 3
1.1.4 Working Mechanism 3
1.1.5 Protocols and Standards 4
1.2 Configuration Task Summary 4
1.3 Configuring Basic IGMP Snooping Functions 5
1.3.1 Overview 5
1.3.2 Restrictions and Guidelines 5
1.3.3 Configuration Tasks 6
1.3.4 Configuring Basic IGMP Snooping Functions in IVGL Mode 6
1.3.5 Configuring Basic IGMP Snooping Functions in SVGL Mode 6
1.3.6 Configuring Basic IGMP Snooping Functions in IVGL-SVGL Mode 7
1.4 Configuring Protocol Packet Processing Parameters 8
1.4.1 Overview 8
1.4.2 Restrictions and Guidelines 9
1.4.3 Configuration Tasks 9
1.4.4 Configuring a Static Multicast Router Port 9
1.4.5 Configuring a Static Member Port 10
1.4.6 Configuring Report Packet Suppression 10
1.4.7 Configuring Port Fast Leave 11

1.4.1 Configuring Dynamic Multicast Router Port Learning 11

1.4.2 Configuring the Aging Time for Dynamic Multicast Router Ports 12

1.4.3 Configuring the Aging Time for Dynamic Member Ports 12

1.5 Configuring IGMP Snooping Querier 13

1.5.1 Overview 13

1.5.2 Restrictions and Guidelines 13

1.5.3 Prerequisites 13

1.5.4 Configuration Tasks 14

1.5.5 Enabling IGMP Snooping Querier 14

1.5.6 Configuring the Source IP Address of a Querier 14

1.5.7 Configuring the IGMP Snooping Querier Version 15

1.5.8 Configuring the Maximum Response Time for Query Packets 15

1.5.9 Configuring the Interval for a Querier to Send Query Packets 16

1.5.10 Configuring the Querier Aging Time 16

1.6 Configuring Multicast Security Control 17

1.6.1 Overview 17

1.6.2 Prerequisites 17

1.6.3 Configuration Tasks 17

1.6.4 Configuring a Profile 17

1.6.5 Configuring a Range of Multicast Group Addresses for a Profile 18

1.6.6 Configuring Multicast Preview 19

1.6.7 Configuring the Maximum Number of Multicast Groups Allowed for Concurrent Request 20

1.6.8 Configuring Source Port Check 21

1.6.9 Configuring Source IP Address Check 21

1.7 Configuring QinQ Processing 22

1.7.1 Overview 22

1.7.2 Restrictions and Guidelines 23

1.7.3 Prerequisites 23

1.7.4 Procedure 23

1.8 Monitoring 23

1.9 Configuration Examples 24

1.9.1 Configuring Basic IGMP Snooping Functions in IVGL Mode 24

1.9.2 Configuring Basic IGMP Snooping Functions in SVGL Mode 29

1.9.3 Configuring Basic IGMP Snooping Functions in IVGL-SVGL Mode 34

1.9.4 Configuring Static Ports to Implement L2 Multicast 42

1.9.5 Configuring IGMP Snooping Querier 47

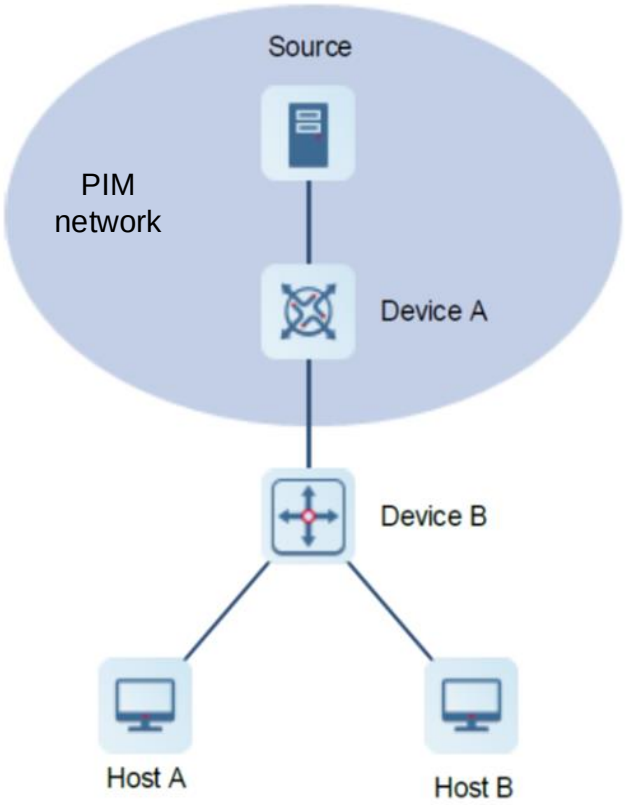
1 Configuring IGMP Snooping

1.1 Introduction

Internet Group Management Protocol (IGMP) snooping is a process of snooping protocol packets between an L3 multicast device and hosts to manage and control forwarding of IP multicast traffic at the data link layer, implementing L2 multicast.

Generally, multicast packets need to pass through L2 switches, especially in some local area networks (LANs). As shown in Figure 1-1, the Protocol Independent Multicast (PIM) multicast device sends packets to hosts through an L2 switch. Because multicast group addresses cannot be learned on L2 devices, the packets will be broadcast in the VLAN. This wastes bandwidth and affects security. After the IGMP snooping function is configured, the L2 switch can listen to IGMP packets between hosts and the uplink PIM multicast device and establish L2 multicast forwarding entries to ensure that multicast data is forwarded only to specific hosts. This prevents multicast data from being broadcast in the L2 network.

Figure 1-1 Network Topology



1.1.2 Principles

IGMP snooping is a basic L2 multicast function that forwards and controls multicast data at the data link layer. By listening to and analyzing protocol packets between hosts and the L3 multicast device, the L2 device

running IGMP snooping establishes and maintains L2 multicast forwarding entries to ensure on-demand forwarding of multicast data at the link layer.

As shown in Figure 1-2, when IGMP snooping is not configured on the L2 device, IP multicast packets are broadcast in the VLAN. As shown in Figure 1-3, when IGMP snooping is enabled on the L2 device, IP multicast packets are forwarded only to the member hosts of the multicast group. This prevents multicast data from being broadcast in the L2 network.

Figure 1-2 Multicast Data Transmission When IGMP Snooping Is Disabled

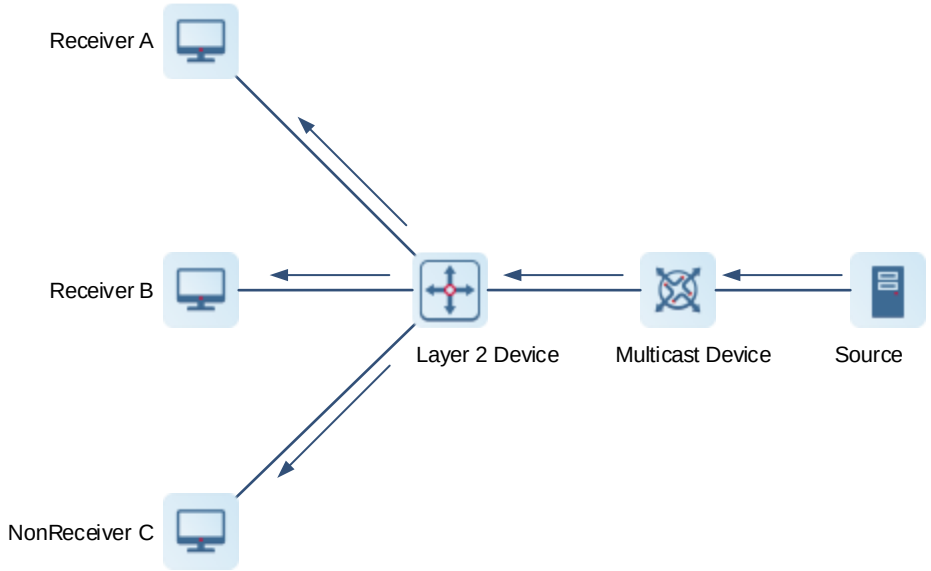
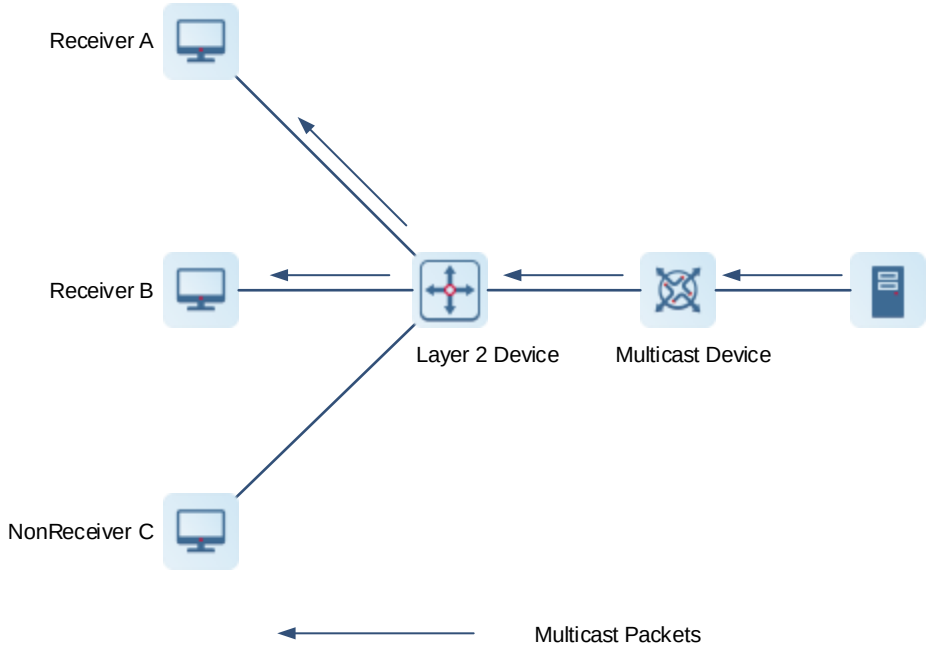


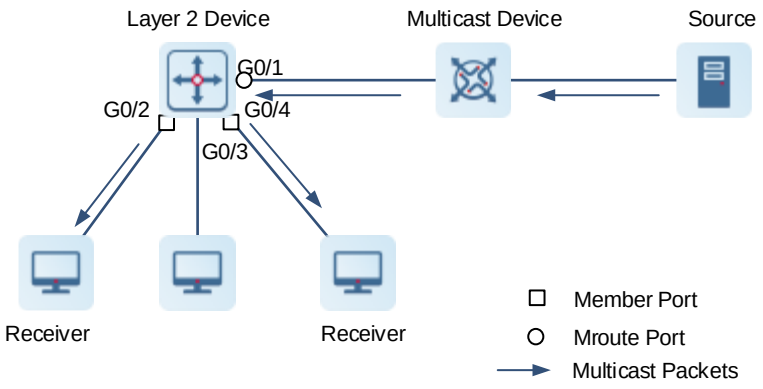
Figure 1-3 Multicast Data Transmission When IGMP Snooping Is Enabled



1.1.3 Port Types

IGMP snooping is enabled on a per-VLAN basis. IGMP snooping ports are ports in a VLAN. The device running IGMP snooping identifies ports in a VLAN as multicast router ports or member ports to manage and control forwarding of IP multicast data in the VLAN.

Figure 1-4 IGMP Snooping Ports



- A multicast router port connects the L2 multicast device to an L3 multicast device, and indicates the direction of the multicast source. By listening to IGMP packets, the L2 multicast device can automatically discover and maintain dynamic multicast router ports. You can also configure static multicast router ports.
- A member port connects the L2 multicast device to a host in a multicast group, and indicates the direction of a multicast group member. It is also called a listener port. By listening to IGMP packets, the L2 multicast device can automatically discover and maintain dynamic member ports. You can also configure static member ports.

As shown in Figure 1-4, IGMP snooping is enabled on the L2 multicast device, and the multicast data is received from a multicast router port and sent out from a member port.

1.1.4 Working Mechanism

A device running IGMP snooping analyzes received IGMP packets to discover and identify multicast router ports and member ports and establish and maintain IGMP snooping forwarding entries. The device can identify and process the following types of IGMP packets:

1. Query Packets

The IGMP querier periodically sends a general Query packet, and sends a group-specific Query packet when it receives a Leave packet. When the device running IGMP snooping receives a Query packet, the device performs the following actions in the VLAN:

- The device forwards the IGMP Query packet through all ports (except the port receiving the packet).
- If the port receiving the Query packet is a dynamic multicast router port, the device resets the aging timer of the port. After the timer times out, the port is no longer used as a dynamic multicast router port.
- If the port receiving the Query packet is not a dynamic multicast router port, the device uses the port as the dynamic multicast router port and starts the aging timer. After the timer times out, the port is no longer used as a dynamic multicast router port.

- If the function of dynamical multicast router port learning is disabled, the device will not learn dynamic multicast router ports.

2. Report Packets

When a member host receives a Query packet, the host will respond with a Report packet. If a host wants to join a multicast group, the host will proactively send a Report packet. The device running IGMP snooping can process IGMPv1 and IGMPv2 packets by default. For Report packets of IGMPv3, the device only processes the group information and does not process the carried source information.

When the device running IGMP snooping receives a Report packet, the device performs the following actions in the VLAN:

- The device forwards the Report packet through all multicast router ports. If Report packet suppression is enabled on the device, the device forwards only the first Report packet of each group in an IGMP query interval.
- If the port receiving the Report packet is a dynamic member port, the device resets the aging timer of the port. After the timer times out, the port is no longer used as a dynamic member port.
- If the port receiving the Report packet is not a member port, the device uses the port as the dynamic member port and starts the aging timer. After the timer times out, the port is no longer used as a dynamic member port.

3. Leave Packets

If a host wants to leave a multicast group, the host will proactively send a Leave packet. When the device running IGMP snooping receives a Leave packet, the device performs the following actions in the VLAN:

- The device forwards the Leave packet through all multicast router ports.
- If the port receiving the Leave packet is a dynamic member port and the fast leave function is configured, the device immediately deletes the port from the IGMP snooping forwarding entry of the corresponding multicast group. The port is no longer used as a dynamic member port of the group.
- If the port receiving the Leave packet is a dynamic member port but the fast leave function is not configured, the port status remains unchanged. When the aging timer of the port times out, the device deletes the port from the IGMP snooping forwarding entry of the corresponding multicast group. The port is no longer used as a dynamic member port of the group.

1.1.5 Protocols and Standards

- RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

1.2 Configuration Task Summary

IGMP snooping configuration includes the following tasks:

(1) Configuring Basic IGMP Snooping Functions. Select either of the following configuration tasks to configure.

- Configuring Basic IGMP Snooping Functions in IVGL Mode
- Configuring Basic IGMP Snooping Functions in SVGL Mode
- Configuring Basic IGMP Snooping Functions in IVGL-SVGL Mode

(2) Configuring Protocol Packet Processing Parameters. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Static Multicast Router Port
- Configuring a Static Member Port
- Configuring Report Packet Suppression
- Configuring Port Fast Leave
- Configuring Dynamic Multicast Router Port Learning
- Configuring the Aging Time for Dynamic Multicast Router Ports
- Configuring the Aging Time for Dynamic Member Ports

(3) (Optional) Configuring IGMP Snooping Querier. The tasks are as follows:

- Enabling IGMP Snooping Querier
- Configuring the Source IP Address of a Querier
- (Optional) Configuring the IGMP Snooping Querier Version
- (Optional) Configuring the Maximum Response Time for Query Packets
- (Optional) Configuring the Interval for a Querier to Send Query Packets
- (Optional) Configuring the Querier Aging Time

(4) Configuring Multicast Security Control. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Profile
- Configuring a Range of Multicast Group Addresses for a Profile
- Configuring Multicast Preview
- Configuring the Maximum Number of Multicast Groups Allowed for Concurrent Request
- Configuring Source Port Check
- Configuring Source IP Address Check

(5) (Optional) Configuring QinQ Processing

1.3 Configuring Basic IGMP Snooping Functions

1.3.1 Overview

The device running IGMP snooping can provide independent or shared multicast services for user VLANs when operated in the following modes:

- Independent VLAN Group Learning (IVGL): provides independent multicast services for each user VLAN.
- Shared VLAN Group Learning (SVGL): provides shared multicast services for multiple user VLANs.
- IVGL-SVGL: provides both shared and independent multicast services for user VLANs.

1.3.2 Restrictions and Guidelines

- The SVGL mode and the IP multicast function are mutually exclusive. If the IP multicast function needs to be enabled on the device running IGMP snooping, the device can operate only in IVGL mode.

- If the device running IGMP snooping operates in SVGL or IVGL-SVGL mode, the multicast groups associated with the SVGL mode must be configured. First, define the multicast groups applied in the SVGL mode in a profile. Then, apply this profile in the command for configuring the group range in SVGL mode.

1.3.3 Configuration Tasks

Basic IGMP snooping function configuration includes the following tasks. Please configure only one task.

- Configuring Basic IGMP Snooping Functions in IVGL Mode
- Configuring Basic IGMP Snooping Functions in SVGL Mode
- Configuring Basic IGMP Snooping Functions in IVGL-SVGL Mode

1.3.4 Configuring Basic IGMP Snooping Functions in IVGL Mode

1. Overview

In IVGL mode, the device running IGMP snooping provides independent multicast services for each user VLAN. Multicast traffic can be forwarded only in the belonged VLAN, and hosts can request multicast traffic only in the belonged VLAN.

2. Restrictions and Guidelines

- Unless otherwise specified, you are advised to enable IGMP snooping globally on all L2 access devices connecting to hosts.
- After IGMP snooping is enabled globally, it takes effect to all VLANs. You can disable IGMP snooping on any VLAN. When the multicast service is disabled on a VLAN, the multicast services on other VLANs are not affected.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IGMP snooping globally and run the IVGL mode.

ip igmp snooping ivgl

IGMP snooping is disabled by default.

(4) (Optional) Disable IGMP snooping on a VLAN.

no ip igmp snooping vlan *vlan-id*

After IGMP snooping is enabled globally, it takes effect to all VLANs by default.

If IGMP snooping is disabled globally, it is ineffective on all VLANs.

You can disable IGMP snooping on a VLAN only after IGMP snooping is enabled globally.

1.3.5 Configuring Basic IGMP Snooping Functions in SVGL Mode

1. Overview

In SVGL mode, the device running IGMP snooping can provide shared multicast services for multiple user VLANs. Shared multicast services are usually used to provide the same video on demand (VOD) service for

users in multiple VLANs. Compared with independent multicast services, shared multicast services save bandwidth.

VLANs for shared multicast services are classified into a shared VLAN and sub VLANs. Multicast traffic of multicast groups applied in SVGL mode on the shared VLAN is forwarded from the shared VLAN to sub VLANs, and hosts on sub VLANs request multicast traffic of multicast groups applied in SVGL mode from the shared VLAN.

2. Restrictions and Guidelines

- To share multicast services among VLANs, you need to configure multicast groups applied in SVGL mode after configuring the SVGL mode.
- Shared multicast services apply only to the shared VLAN and sub VLANs and use group addresses applied in SVGL mode.

3. Prerequisites

Before configuring multicast groups associated with the SVGL mode, ensure that the corresponding profile is created and a range of multicast groups that are permitted or denied by the filter is specified. For details about profile configuration, see 1.6.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IGMP snooping globally and run the SVGL mode.

ip igmp snooping svgl

IGMP snooping is disabled by default.

(4) Configure multicast groups associated with the SVGL mode.

ip igmp snooping svgl profile *profile-number*

No multicast group is associated with the SVGL mode by default.

(5) (Optional) Specify a shared VLAN.

ip igmp snooping svgl vlan *vlan-id*

The default shared VLAN in SVGL mode is VLAN 1.

(6) (Optional) Specify sub VLANs in SVGL mode.

ip igmp snooping svgl subvlan *vlan-range*

By default, all VLANs except the shared VLAN are sub VLANs in SVGL mode.

1.3.6 Configuring Basic IGMP Snooping Functions in IVGL-SVGL Mode

1. Overview

The IVGL-SVGL mode is also called the hybrid mode. In IVGL-SVGL mode, the device running IGMP snooping can provide both shared and independent multicast services for user VLANs.

- In the shared VLAN and sub VLANs, shared multicast services apply to the multicast traffic of multicast

groups applied in SVGL mode, and independent multicast services apply to other multicast traffic.

- In other VLANs (except the shared VLAN and sub VLANs), independent multicast services are provided.

2. Restrictions and Guidelines

- After configuring the IVGL-SVGL mode, you must specify the multicast groups associated with the SVGL mode.
- When a user VLAN is configured as a shared VLAN or sub VLAN, the user VLAN enjoys both shared and independent multicast services. When a user VLAN is configured as other VLANs, it enjoys only independent multicast services.

3. Prerequisites

Before configuring multicast groups associated with the SVGL mode, ensure that the corresponding profile is created and a range of multicast groups that are permitted or denied by the filter is specified. For details about profile configuration, see 1.6.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IGMP snooping globally and run the IVGL-SVGL mode.

ip igmp snooping ivgl-svgl

IGMP snooping is disabled by default.

(4) Configure multicast groups associated with the SVGL mode.

ip igmp snooping svgl profile *profile-number*

No multicast group is associated with the SVGL mode by default.

(5) (Optional) Specify a shared VLAN.

ip igmp snooping svgl vlan *vlan-id*

The default shared VLAN in SVGL mode is VLAN 1.

(6) (Optional) Specify sub VLANs in SVGL mode.

ip igmp snooping svgl subvlan *vlan-range*

All VLANs except the shared VLAN are sub VLANs in SVGL mode by default.

1.4 Configuring Protocol Packet Processing Parameters

1.4.1 Overview

By controlling protocol packet processing, an L2 multicast device can establish static or dynamic multicast forwarding entries. In addition, the device can adjust parameters to refresh dynamic multicast forwarding entries and IGMP snooping membership quickly.

1.4.2 Restrictions and Guidelines

Configuring Basic IGMP Snooping Functions Related configuration functions take effect only after basic IGMP snooping functions are configured.

1.4.3 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Static Multicast Router Port
- Configuring a Static Member Port
- Configuring Report Packet Suppression
- Configuring Port Fast Leave
- Configuring Dynamic Multicast Router Port Learning
- Configuring the Aging Time for Dynamic Multicast Router Ports
- Configuring the Aging Time for Dynamic Member Ports

1.4.4 Configuring a Static Multicast Router Port

1. Overview

A multicast router port is used to receive uplink multicast data and forward IGMP Report and Leave packets. Static multicast router ports never age and can forward IGMP Report and Leave packets to the uplink IGMP querier stably.

2. Restrictions and Guidelines

- In SVGL mode, if no sub VLAN is configured, the configuration of static multicast router ports is valid only in the shared VLAN. In other VLANs, static multicast router ports can be configured but do not take effect. If sub VLANs are configured, the configuration of static multicast router ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static multicast router ports can be configured but do not take effect.
- In SVGL-IVGL mode, if no sub VLAN is configured, the configuration of static multicast router ports is valid in all VLANs. If sub VLANs are configured, the configuration of static multicast router ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static multicast router ports can be configured but do not take effect.
- In IVGL mode, the configuration of static multicast router ports is valid in all VLANs.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static multicast router port.

ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-type interface-number*

No static multicast router port is configured by default.

1.4.5 Configuring a Static Member Port

1. Overview

When a member port connecting to a member host is configured as a static member port, the host can receive multicast traffic from the specified multicast group no matter whether the host joins the multicast group. Static member ports never age.

2. Restrictions and Guidelines

- In SVGL mode, if no sub VLAN is configured, the configuration of static member ports is valid only in the shared VLAN. In other VLANs, static member ports can be configured but do not take effect. If sub VLANs are configured, the configuration of static member ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static member ports can be configured but do not take effect.
- In SVGL-IVGL mode, if no sub VLAN is configured, the configuration of static member ports is valid in all VLANs. If sub VLANs are configured, the configuration of static member ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static member ports can be configured but do not take effect.
- In IVGL mode, the configuration of static member ports is valid in all VLANs.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static member port.

ip igmp snooping vlan *vlan-id* **static** *group-address* **interface** *interface-type interface-number*

No static member port is configured by default.

1.4.6 Configuring Report Packet Suppression

1. Overview

IGMP Query and Report packets are exchanged periodically to maintain the group membership. When many hosts in a network join the same multicast group, a large number of IGMP packets will be sent to the IGMP multicast device, which wastes network bandwidth and affects the performance of the IGMP multicast device. Report packet suppression can optimize this situation.

When Report packet suppression is configured, the IGMP multicast device only forwards the first Report packet from a specific VLAN for a multicast group to the multicast router port and suppresses subsequent Report packets for the same multicast group during one query interval. This function reduces the number of packets in the network.

2. Restrictions and Guidelines

Only IGMPv1 and IGMPv2 Report packets can be suppressed, and IGMPv3 Report packets cannot be suppressed.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure Report packet suppression.

ip igmp snooping suppression enable

Report packet suppression is disabled by default.

1.4.7 Configuring Port Fast Leave

1. Overview

When the port fast leave function is enabled and a port receives a Leave packet (including the IGMPv2 Leave packet and IGMPv3 Report packet of the INCLUDE type without carrying any source address), the port is directly deleted from the member port list of the corresponding multicast forwarding entry. When receiving group-specific Query packets and multicast data, the device does not forward the packets to this port.

2. Restrictions and Guidelines

The port fast leave function is applicable when only one host is connected to each port. This function helps save bandwidth and resources.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the port fast leave function.

ip igmp snooping fast-leave enable

The port fast leave function is disabled by default.

1.4.1 Configuring Dynamic Multicast Router Port Learning

1. Overview

In some application scenarios, a user host may send Query packets and PIM neighbor messages. When the L2 device receives such Query packets or PIM neighbor messages, the L2 device will set the port receiving the packets as a dynamic multicast router port. All multicast packets in the VLAN will be forwarded to this port, and the host receives a large number of useless multicast packets. In addition, Query packets and PIM neighbor messages sent by user hosts may affect the status of the L3 multicast routing protocol, such as the querier and designated router (DR) election. In this case, you can disable dynamic multicast router port learning to resolve this problem and improve network security.

2. Restrictions and Guidelines

Disabling dynamic multicast router port learning and enabling a static multicast router port do not affect each other.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure dynamic multicast router port learning.

ip igmp snooping [**vlan** *vlan-id*] **mrouter learn pim-dvmrp**

Dynamic multicast router port learning is enabled by default.

1.4.2 Configuring the Aging Time for Dynamic Multicast Router Ports

1. Overview

A multicast router port is used to receive uplink multicast data and forward IGMP Report and Leave packets. After enabling IGMP snooping, an L2 device can dynamically learn multicast router ports to forward multicast packets for the unplink device. If a dynamic multicast router port does not receive a Query packet or neighbor message from the uplink device within the aging time due to unstable network or packet congestion, the L2 device will delete the dynamic multicast router port, which may cause multicast data interruption.

2. Restrictions and Guidelines

- You can adjust the aging time of dynamic multicast router ports based on the network load. When the network load is heavy, set the aging time to a larger value. A too short aging time may cause dynamic multicast router ports to be added and deleted frequently, resulting in data interruption.
- You can set the aging time based on the interval for the connected multicast router to send IGMP Query packets. Generally, the aging time is set to twice the interval plus the response time of the last IGMP Query packet.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the aging time for dynamic multicast router ports.

ip igmp snooping dyn-mr-aging-time *dynamic-mroute-aging-time*

The default aging time of dynamic multicast router ports is 300s.

1.4.3 Configuring the Aging Time for Dynamic Member Ports

1. Overview

When the device running IGMP snooping receives an IGMP Join packet from a host to join an IP multicast group, the device adds the port receiving the packet to the member port list and sets an aging time for the port. If the port is already in the member port list, the device resets the aging timer of the port. After the timer times out, it is deemed that no user host receives multicast packets through this port, and the multicast device deletes the port from the IGMP snooping member port list.

2. Restrictions and Guidelines

- You can adjust the aging time of dynamic member ports based on the network load. When the network load is heavy, set the aging time to a larger value. A too short aging time may cause dynamic member ports to be added and deleted frequently, resulting in data interruption.
- After the aging time is configured, the aging timer value of dynamic member ports is *host-aging-time* for subsequent IGMP Join packets. The configured aging time takes effect after the next Join packet is received, and the started member port aging timers are not updated.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the aging time for dynamic member ports.

ip igmp snooping host-aging-time *host-aging-time*

The default aging time of dynamic member ports is 260s.

1.5 Configuring IGMP Snooping Querier

1.5.1 Overview

In a three-layer multicast network, the L3 multicast device serves as the querier and runs IGMP to maintain group membership. The L2 multicast device only needs to listen to IGMP packets to establish and maintain multicast forwarding entries, implementing L2 multicast. When a multicast source and user host are in the same L2 network, the query function is unavailable because the L2 device does not support IGMP. To resolve this problem, you can enable the IGMP snooping querier function on the L2 device so that the L2 device sends IGMP Query packets to user hosts on behalf of the L3 multicast device, and listens to and maintains IGMP Report packets responded by user hosts to establish L2 multicast forwarding entries. When multiple devices are configured as the querier in the L2 network and a device receives IGMP Query packets from other devices, an IGMP snooping querier is elected.

1.5.2 Restrictions and Guidelines

- After the querier function is enabled, you must specify a source IP address for the querier so that the querier function can take effect.
- When a device with the querier function enabled receives a PIM or Distance Vector Multicast Routing Protocol (DVMRP) packet, it regards that a multicast router exists in the network. To prevent the IGMP routing function of the multicast router from being affected, the querier function of the device becomes invalid and the multicast router in the network serves as the IGMP snooping querier.
- The query interval configured for the querier must be greater than the maximum response time of Query packets. Otherwise, the configuration fails.

1.5.3 Prerequisites

Configuring Basic IGMP Snooping Functions

1.5.4 Configuration Tasks

IGMP snooping querier configuration includes the following tasks:

- Enabling IGMP Snooping Querier
- Configuring the Source IP Address of a Querier
- (Optional) Configuring the IGMP Snooping Querier Version
- (Optional) Configuring the Maximum Response Time for Query Packets
- (Optional) Configuring the Interval for a Querier to Send Query Packets
- (Optional) Configuring the Querier Aging Time

1.5.5 Enabling IGMP Snooping Querier

1. Overview

After the IGMP snooping querier function is enabled on an L2 device, the L2 device sends IGMP Query packets to user hosts on behalf of the L3 device.

2. Restrictions and Guidelines

- The IGMP snooping querier function must be enabled globally and on a specific VLAN. The IGMP snooping querier function on a specific VLAN takes effect only after the function is enabled globally.
- You can disable the IGMP snooping querier function for a specific VLAN.
- If the IGMP snooping querier function is disabled globally, the function is disabled on all VLANs.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IGMP snooping querier function.

ip igmp snooping [**vlan** *vlan-id*] **querier**

The IGMP snooping querier function is disabled by default.

1.5.6 Configuring the Source IP Address of a Querier

1. Overview

You can configure the source IP address of a querier globally or on a specific VLAN. If the source IP address of the querier is not configured, the querier function does not take effect.

2. Restrictions and Guidelines

The querier source IP address configured on a specific VLAN, if any, prevails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the source IP address of a querier.

ip igmp snooping [**vlan** *vlan-id*] **querier address** *source-address*

By default, no VLAN is specified, and the source IP address configuration applies to all VLANs.

1.5.7 Configuring the IGMP Snooping Querier Version

1. Overview

You can configure the IGMP snooping querier version to specify the version of IGMP Query packets sent by the querier. The supported IGMP versions include IGMPv1and IGMPv2.

2. Restrictions and Guidelines

- An IGMP snooping querier supports IGMPv1and IGMPv2, and IGMPv2 is used by default. You can run the corresponding command to enable an IGMP snooping querier to run IGMPv1 or IGMPv3.
- The IGMP snooping querier version configured on a specific VLAN, if any, prevails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the IGMP snooping querier version.

ip igmp snooping [**vlan** *vlan-id*] **querier version 1**

An IGMP snooping querier runs IGMPv2 by default.

1.5.8 Configuring the Maximum Response Time for Query Packets

1. Overview

When hosts in the directly-connected network segment of the device serving as the IGMP snooping querier receive a Query packet from the device, the hosts need to return a Report packet within the maximum response time. This function allows you to configure the maximum response time for Query packets on the device. If no host returns a Report packet within the maximum response time, the device considers that no group member exists in the directly-connected network segment and deletes the group information.

2. Restrictions and Guidelines

- You can adjust the maximum response time for Query packets based on the network load. When the network load is light, you are advised to set the maximum response time for Query packets to a small value to enable hosts to make quick responses to IGMP Query packets. When the network load is heavy, set a large maximum response time to avoid network congestion due to flooding of Report packets sent by hosts after the timer times out.
- Because IGMPv1 does not support carrying the maximum response time in packets, this configuration does not take effect to a querier running IGMPv1.

- You can configure different maximum response time values for queriers in different VLANs. The maximum response time configured on a specific VLAN, if any, prevails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum response time for Query packets.

ip igmp snooping [**vlan** *vlan-id*] **querier max-response-time** *max-response-time*

The maximum response time for Query packets is 10s by default.

1.5.9 Configuring the Interval for a Querier to Send Query Packets

1. Overview

An IGMP snooping querier periodically sends Query packets. This parameter is used to define the interval for sending Query packets.

2. Restrictions and Guidelines

You can configure the interval for a querier to send Query packets globally or on a specific VLAN. The query interval specified on a VLAN, if any, prevails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the interval for a querier to send Query packets.

ip igmp snooping [**vlan** *vlan-id*] **querier query-interval** *query-interval*

The default interval for an IGMP snooping querier to send Query packets is 60s.

1.5.10 Configuring the Querier Aging Time

1. Overview

When multiple queriers are configured in an L2 network, querier election will be performed, and the device elected as the querier will send Query packets periodically. Other candidate queriers receive Query packets from the elected querier. If a candidate querier does not receive Query packets from the elected querier within a specific period of time, the candidate querier regards that it is the only querier in the directly-connected network segment and initiates a new round querier election. This parameter is used to define the timeout time for candidate queriers to receive Query packets from the elected querier.

2. Restrictions and Guidelines

The querier aging time configured on a specific VLAN, if any, prevails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the querier aging time.

ip igmp snooping [**vlan** *vlan-id*] **querier timer expiry** *timeout*

The default aging time of IGMP snooping queriers is 125s.

1.6 Configuring Multicast Security Control

1.6.1 Overview

After multicast security control is configured, the device running IGMP snooping can control the multicast service scope and load to prevent invalid multicast traffic and improve L2 multicast network security.

1.6.2 Prerequisites

Configuring Basic IGMP Snooping Functions

1.6.3 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Profile
- Configuring a Range of Multicast Group Addresses for a Profile
- Configuring Multicast Preview
- Configuring the Maximum Number of Multicast Groups Allowed for Concurrent Request
- Configuring Source Port Check
- Configuring Source IP Address Check

1.6.4 Configuring a Profile

1. Overview

A profile is used to define a range of multicast groups that permit or deny user access for reference by other functions.

- When the SVGL mode is enabled, a profile is used to define a range of multicast groups applied in SVGL mode.
- When multicast filtering is configured on a port, a profile is used to define a range of multicast groups that permit or deny user access through the port.
- When multicast filtering is configured on a VLAN, a profile is used to define a range of multicast groups that permit or deny user access on the VLAN.
- When the preview function is enabled, a profile is used to define a range of multicast groups to be previewed.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a profile.

ip igmp profile *profile-number*

No profile is created by default.

(4) Define a range of multicast groups for a profile.

range *low-ip-address* [*high-ip-address*]

No multicast group range is defined for a profile by default.

Multiple multicast group ranges can be configured at the same time. If two multicast group ranges overlap, the ranges will be merged automatically.

(5) Configure the filtering action for a profile. The configuration steps below are mutually exclusive. Please configure only one task.

- Set the filtering action of a profile to Deny.

  deny

  If only the Deny action is configured and no multicast group range is configured, no group is denied. The effect is the same as permitting all groups.

- (Optional) Set the filtering action of a profile to Permit.

  permit

  If only the Permit action is configured and no multicast group range is configured, no group is permitted. The effect is the same as denying all groups.

The Deny action is performed for a profile by default.

1.6.5 Configuring a Range of Multicast Group Addresses for a Profile

1. Overview

Generally, the device running ports and VLANs can join any multicast group. By configuring a range of multicast groups that permit or deny user access, you can customize the multicast service scope for users to guarantee the interest of operators and prevent invalid multicast traffic.

2. Restrictions and Guidelines

- By applying a profile to a VLAN, you can restrict the multicast groups that users can join in the VLAN.
- By applying a profile to a port, you can restrict the multicast groups that users can join on the port.

3. Prerequisites

Before configuring a range of multicast group addresses for a profile, ensure that the corresponding profile is created and a range of multicast groups is specified for the profile. For details about profile configuration, see 1.6.4 Configuring a Profile.

4. Procedure

Configure a range of multicast groups for a profile. Select at least one of them to configure.

- Apply a profile for a port.

  a Enter the privileged EXEC mode.

  enable

  b Enter the global configuration mode.

  configure terminal

  c Enter the interface configuration mode.

  interface *interface-type interface-number*

  d Apply a profile to a port.

  ip igmp snooping filter *profile-number*

  No profile is applied to a port by default.

- Apply a profile to a VLAN.

  a Enter the privileged EXEC mode.

  enable

  e Enter the global configuration mode.

  configure terminal

  f Apply a profile to a VLAN.

  ip igmp snooping vlan *vlan-id* **filter** *profile-number*

  No profile is applied to a VLAN by default.

1.6.6 Configuring Multicast Preview

1. Overview

In video applications, the administrator configures a VLAN filter or port filter to control some premium channels. Users who do not subscribe to these channels cannot watch these channels on demand. The multicast preview function allows unpaid users to preview premium channels before they decide whether to pay for watching. This function can be used together with multicast permission control.

2. Restrictions and Guidelines

After the preview duration ends, unpaid users can no longer watch premium channels on demand. The previewed content can be previewed again after 300s.

3. Prerequisites

Before configuring multicast preview, ensure that the corresponding profile is created and a range of multicast groups allowed for preview is specified. For details about profile configuration, see 1.6.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure multicast preview.

ip igmp snooping preview *profile-number*

The multicast preview function is disabled by default.

(4) (Optional) Configure the preview duration.

ip igmp snooping preview interval preview-*interval*

The default multicast preview duration is 60s.

1.6.7 Configuring the Maximum Number of Multicast Groups Allowed for Concurrent Request

1. Overview

If too much multicast traffic is requested concurrently, the multicast device will be severely burdened. Configuring the maximum number of multicast groups allowed for concurrent request can guarantee the bandwidth. You can limit the number of multicast groups allowed for concurrent request globally or on a port.

- Global maximum number of multicast groups allowed for concurrent request: This configuration contains statically configured and dynamically learned multicast groups.
- Maximum number of multicast groups allowed for concurrent request on a port: This configuration contains only dynamically learned multicast groups on a port and does not include statically configured multicast groups.

2. Restrictions and Guidelines

- To limit the number of multicast groups allowed for concurrent request globally, configure the global maximum number of multicast groups allowed for concurrent request.
- To limit the number of multicast groups allowed for concurrent request on a port, configure the maximum number of multicast groups that can be dynamically learned by the port.
- The number of multicast groups that can be dynamically learned by a port is counted based on the VLANs to which the port belongs. For example, if a port belongs to three VLANs and the port receives requests of multicast group 224.1.1.1 from each VLAN, the multicast group count on the port is 3 instead of 1.

3. Procedure

Configure the maximum number of multicast groups allowed for concurrent request. Select at least one of them to configure.

- Configure the maximum number of multicast groups allowed for concurrent request globally.

  a Enter the privileged EXEC mode.

  enable

  b Enter the global configuration mode.

  configure terminal

  c Configure the maximum number of multicast groups allowed for concurrent request globally.

  ip igmp snooping l2-entry-limit *l2-entry-limit*

  The maximum number of multicast groups allowed for concurrent request globally is 64,000 by default.

- Configure the maximum number of multicast groups that can be dynamically learned by a port.

a Enter the privileged EXEC mode.

enable

d Enter the global configuration mode.

configure terminal

e Enter the interface configuration mode.

interface *interface-type interface-number*

f Configure the maximum number of multicast groups that can be dynamically learned by a port.

ip igmp snooping max-groups *max-groups*

The maximum number of multicast groups that can be dynamically learned by a port is 64,000 by default.

1.6.8 Configuring Source Port Check

1. Overview

The source port check function restricts users to receive only multicast traffic on multicast router ports to prevent users from sending invalid multicast traffic.

- After the source port check function is enabled, only multicast traffic received on multicast router ports is valid. Multicast traffic received on other ports is invalid and will be discarded.
- When the source port check function is disabled, multicast traffic received on any port is valid.

2. Restrictions and Guidelines

- To restrict users to receive multicast traffic only on multicast router ports, configure this function.
- If no multicast router port exists after the source port check function is enabled, the device will discard received multicast traffic.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure source port check.

ip igmp snooping source-check port

Source port check is disabled by default.

1.6.9 Configuring Source IP Address Check

1. Overview

The source IP address check function strictly restricts the source IP address of multicast traffic to prevent invalid multicast traffic.

Source IP address check contains the following two configurations:

- Default source IP address check: A source IP address is specified for each multicast group in all VLANs. Only multicast traffic with the source IP address the same as the preset one is valid.

- Group-specific source IP address check: A source IP address is specified for a specific multicast group in a specific VLAN. The multicast device forwards only data traffic of the specific multicast group received in the VLAN that has the same source IP address as the preset one and discards other multicast traffic from the specific multicast group.

2. Restrictions and Guidelines

- When source IP address check is enabled or disabled, all multicast forwarding entries on the L2 device will be deleted and the device needs to learn entries in the next query interval.
- Group-specific source IP address check can be configured only after default source IP address check is configured.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure default source IP address check.

ip igmp snooping source-check default-server *source-address*

Source IP address check is disabled by default.

(4) Configure group-specific source IP address check.

ip igmp snooping limit-ipmc vlan *vlan-id* **address** *group-address* **server** *source-address*

Only the multicast source address is checked by default.

1.7 Configuring QinQ Processing

1.7.1 Overview

On a device with IGMP snooping enabled and a dot1q-tunnel (QinQ) port configured, IGMP snooping will process the IGMP packets received on the QinQ port using the following two modes:

- Mode 1: Create multicast entries on the VLAN where the IGMP packets are located. Forwarding IGMP packets on the VLAN where these packets are located is called transparent transmission. For example, IGMP snooping is enabled for a device, Port A on the device is designated as the QinQ port, the default VLAN of this port is VLAN 1, and Port A allows the passage of VLAN 1 and VLAN 10 packets. When an IGMP Report packet is sent from VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 10 and forwards the IGMP Report packet to the multicast router port of VLAN 10.
- Mode 2: Create multicast entries on the default VLAN of the QinQ port. Encapsulate the IGMP packets with the VLAN tag of the default VLAN where the QinQ port is located and forward the packets within the default VLAN. For example, IGMP snooping is enabled for a device, Port A on the device is designated as the QinQ port, the default VLAN of this port is VLAN 1, and Port A allows the passage of VLAN 1 and VLAN 10 packets. When an IGMP Report packet is sent from VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 1, encapsulates the IGMP Report packet with the tag of VLAN 1, and forwards the packet to the multicast router port of VLAN 1.

IGMP snooping works in mode 2 by default. You can run the **ip igmp snooping tunnel** command to enable IGMP snooping to work in mode 1.

1.7.2 Restrictions and Guidelines

If the QinQ port needs to forward multicast packets on the VLANs specified by the VLAN IDs (VIDs) of the packets, transparent packet transmission needs to be configured on the QinQ port.

1.7.3 Prerequisites

- Configuring Basic IGMP Snooping Functions
- Configure basic QinQ functions. For details about QinQ configuration, see "Configuring QinQ" in the *Ethernet Switching Configuration Guide*.

1.7.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure transparent packet transmission on the QinQ port.

ip igmp snooping tunnel

The function of transparent IGMP packet transmission on the QinQ port is disabled by default.

1.8 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear ip igmp snooping statistics	Clears IGMP snooping statistics.
clear ip igmp snooping gda-table	Clears dynamic multicast router ports and member ports.
show ip igmp snooping [**vlan** *vlan-id*]	Displays basic IGMP snooping configurations.

Command	Purpose
show ip igmp snooping statistics [**vlan** *vlan-id*]	Displays IGMP snooping statistics.
show ip igmp snooping mrouter	Displays multicast router ports.
show ip igmp snooping gda-table	Displays IGMP snooping forwarding entries.
show ip igmp profile [*profile-number*]	Displays a profile.
show ip igmp snooping interfaces [*interface-type interface-number*]	Displays IGMP snooping configurations on a port.
show ip igmp snooping querier [**detail**]	Displays the IGMP snooping querier.
debug igmp-snp	Debugs all IGMP snooping functions.
debug igmp-snp event	Debugs IGMP snooping events.
debug igmp-snp packet	Debugs IGMP snooping packets.
debug igmp-snp msf	Debugs communication between IGMP snooping and Multicast Source Filter (MSF).
debug igmp-snp warning	Debugs IGMP snooping warnings.

1.9 Configuration Examples

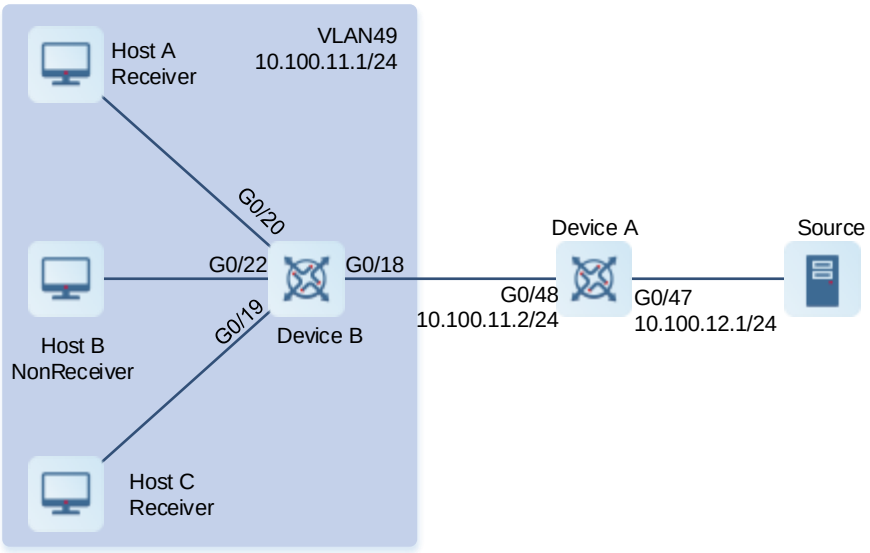
1.9.1 Configuring Basic IGMP Snooping Functions in IVGL Mode

1. Requirements

In the multicast network shown in Figure 1-5, the router (Device A) connects to the user network through the switch (Device B), and IGMP snooping is run on Device A. The multicast source sends data to multicast group 225.0.0.10. There are three hosts (Host A, Host B, and Host C) in the network. Host A and Host C join multicast group 225.0.0.10. Only Host A and Host C can receive multicast data that the multicast source sends to multicast group 225.0.0.10.

2. Topology

Figure 1-5 Topology of Basic IGMP Snooping Functions in IVGL Mode



3. Notes

Configure basic IGMP snooping functions on Device B.

- Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and Protocol Independent Multicast-Sparse Mode (PIM-SM) related functions on Device A.
- Enable IGMP snooping and run the IVGL mode on Device B.

4. Procedure

(1) Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IP address and unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ip address 10.100.12.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# no switchport
DeviceA(config-if-GigabitEthernet 0/48)# ip address 10.100.11.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# router ospf 49
DeviceA(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceA(config-router)# network 10.100.12.0 0.0.0.255 area 0
```

```
DeviceA(config-router)# exit
```

Configure the IP address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan 49
DeviceB(config-vlan)# exit
DeviceB(config)# interface vlan 49
DeviceB(config-if-VLAN 49)#ip address 10.100.11.1 255.255.255.0
DeviceB(config-if-VLAN 49)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# router ospf 49
DeviceB(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceB(config-router)# exit
```

(2) Enable multicast routing and PIM-SM related functions on Device A.

```
DeviceA(config)# ip multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ip pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ip pim rp-candidate GigabitEthernet 0/47
```

(3) Enable IGMP snooping and run the IVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping ivgl
```

5. Verification

Send packets from the multicast source (10.100.12.2) to multicast group G (225.0.0.10). Enable Host A and Host C to join G.

Run the **show ip igmp snooping gda-table** command on Device B to display the IGMP snooping forwarding entry and check whether the member port list contains only GigabitEthernet 0/19 and GigabitEthernet 0/20.

```
DeviceB> enable
DeviceB# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 225.0.0.10, 49):
  VLAN(49) 3 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/19(DM)
    GigabitEthernet 0/20(DM)

DeviceB#
```

Run the **show ip igmp snooping** command on Device B and check whether the IGMP snooping working mode is IVGL.

```
DeviceB# show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 64000
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Global Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Snooping version: 2
IGMP Preview group aging time: 60(Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)

vlan 49
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip multicast-routing
!
```

```
interface GigabitEthernet 0/47
 no switchport
 ip address 10.100.12.1 255.255.255.0
ip pim sparse-mode
!
interface GigabitEthernet 0/48
 no switchport
 ip address 10.100.11.2 255.255.255.0
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.12.0 0.0.0.255 area 0
!
ip pim bsr-candidate GigabitEthernet 0/48
ip pim rp-candidate GigabitEthernet 0/48
!
```

- Device B configuration file

```
hostname DeviceB
!
vlan range 1,49
!
interface GigabitEthernet 0/18
 switchport access vlan 49
!
interface GigabitEthernet 0/19
 switchport access vlan 49
!
interface GigabitEthernet 0/20
 switchport access vlan 49
!
interface GigabitEthernet 0/22
 switchport access vlan 49
!
interface VLAN 49
 ip address 10.100.11.1 255.255.255.0
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
!
ip igmp snooping ivgl
!
```

7. Common Errors

- The working mode of IGMP snooping is improper.

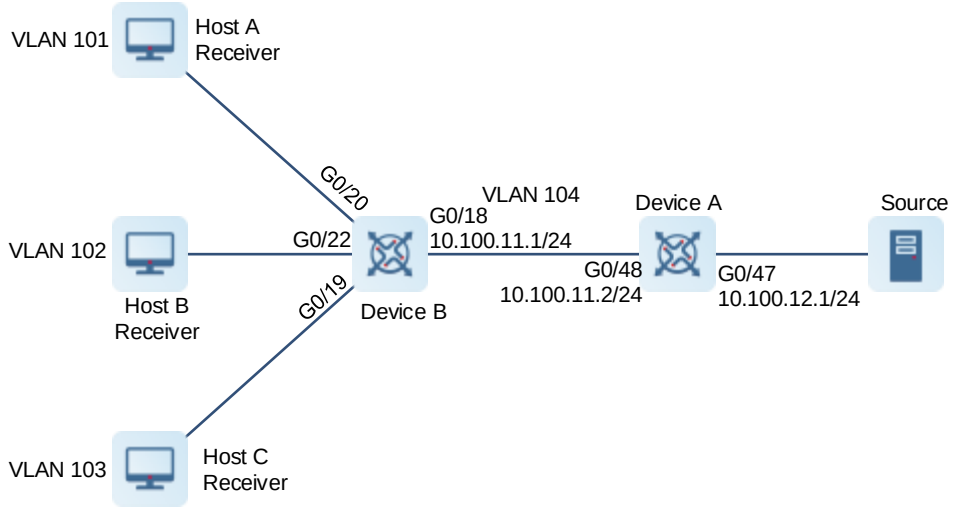
1.9.2 Configuring Basic IGMP Snooping Functions in SVGL Mode

1. Requirements

In the multicast network shown in Figure 1-6, the router (Device A) connects to the user network through the switch (Device B), IGMP snooping is run on Device A, and Device A directly connects to the multicast source. The multicast source sends data to multicast group 225.0.0.10. Host A, Host B, and Host C are connected to VLAN 101, VLAN 102, and VLAN 103, respectively, and the three hosts join multicast group 225.0.0.10. Host A, Host B, and Host C can receive multicast data that the multicast source sends to multicast group 225.0.0.10.

2. Topology

Figure 1-6 Topology of Basic IGMP Snooping Functions in SVGL Mode



3. Notes

Configure basic IGMP snooping functions on Device B.

- Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and PIM-SM related functions on Device A.
- Enable IGMP snooping and run the SVGL mode on Device B.
- Configure the multicast groups associated with the IGMP snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

4. Procedure

(1) Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IP address and unicast routing protocol on Device A.

```
DeviceA> enable
```

```
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ip address 10.100.12.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# vlan 104
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ip address 10.100.11.2 255.255.255.0
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/48)# switchport trunk native vlan 104
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# router ospf 49
DeviceA(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceA(config-router)# network 10.100.12.0 0.0.0.255 area 0
DeviceA(config-router)# exit
```

Configure the IP address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan range 101-104
DeviceB(config-vlan-range)# exit
DeviceB(config)# interface VLAN 101
DeviceB(config-if-VLAN 101)# ip address 10.100.101.1 255.255.255.0
DeviceB(config-if-VLAN 101)# exit
DeviceB(config)# interface VLAN 102
DeviceB(config-if-VLAN 102)# ip address 10.100.102.1 255.255.255.0
DeviceB(config-if-VLAN 102)# exit
DeviceB(config)# interface VLAN 103
DeviceB(config-if-VLAN 103)# ip address 10.100.103.1 255.255.255.0
DeviceB(config-if-VLAN 103)# exit
DeviceB(config)# interface VLAN 104
DeviceB(config-if-VLAN 104)# ip address 10.100.11.1 255.255.255.0
DeviceB(config-if-VLAN 104)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/18)# switchport trunk native vlan 104
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 103
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 101
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 102
```

```
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# router ospf 49
DeviceB(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.101.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.102.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.103.0 0.0.0.255 area 0
DeviceB(config-router)# exit
```

(2) Enable multicast routing and PIM-SM related functions on Device A.

```
DeviceA(config)# ip multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ip pim sparse-mode
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# ip pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ip pim rp-candidate GigabitEthernet 0/47
```

(3) Enable IGMP snooping and run the IVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping svgl
```

(4) Configure the multicast groups associated with the IGMP snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp profile 1
DeviceB(config-profile)# permit
DeviceB(config-profile)# range 224.1.1.1 238.1.1.1
DeviceB(config-profile)# exit
DeviceB(config)# ip igmp snooping svgl profile 1
DeviceB(config)# ip igmp snooping svgl vlan 104
DeviceB(config)# ip igmp snooping svgl subvlan 101-103
```

5. Verification

Send packets from the multicast source (10.100.12.2) to multicast group G (225.0.0.10). Enable Host A, Host B, and Host C to join G.

Run the **show ip igmp snooping gda-table** command on Device B to display the IGMP snooping forwarding entry and check whether the member port list contains GigabitEthernet 0/19, GigabitEthernet 0/20, and GigabitEthernet 0/22.

```
DeviceB> enable
DeviceB# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
```

```
  M: MROUTE
(*, 225.0.0.10, 104):
  VLAN(104) 1 OPORTS:
    GigabitEthernet 0/18(M)

  VLAN(102) 1 OPORTS:
    GigabitEthernet 0/22(D)

  VLAN(103) 1 OPORTS:
    GigabitEthernet 0/19(D)

  VLAN(101) 1 OPORTS:
    GigabitEthernet 0/20(D)

DeviceB#
```

Run the **show ip igmp snooping** command on Device B and check whether the IGMP snooping working mode is SVGL.

```
DeviceB> enable
DeviceB# show ip igmp snooping
IGMP Snooping running mode: SVGL
IGMP Snooping L2-entry-limit: 64000
SVGL vlan: 104
SVGL profile number: 1
IGMP Snooping SVGL subvlan: 101-103
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Global Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Snooping version: 2
IGMP Preview group aging time: 60(Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip multicast-routing
!
vlan 104
!
```

```
interface GigabitEthernet 0/47
 no switchport
 ip address 10.100.12.1 255.255.255.0
ip pim sparse-mode
!
interface GigabitEthernet 0/48
 switchport mode trunk
 switchport trunk native vlan 104
!
interface VLAN 104
 ip address 10.100.11.2 255.255.255.0
ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.12.0 0.0.0.255 area 0
!
ip pim bsr-candidate GigabitEthernet 0/48
ip pim rp-candidate GigabitEthernet 0/48
!
```

- Device B configuration file

```
hostname DeviceB
!
ip igmp profile 1
 permit
 range 224.1.1.1 238.1.1.1
!
vlan range 1,101-104
!
interface GigabitEthernet 0/18
 switchport mode trunk
 switchport trunk native vlan 104
!
interface GigabitEthernet 0/19
 switchport access vlan 103
!
interface GigabitEthernet 0/20
 switchport access vlan 101
!
interface GigabitEthernet 0/22
 switchport access vlan 102
!
interface VLAN 101
 ip address 10.100.101.1 255.255.255.0
!
```

```
interface VLAN 102
 ip address 10.100.102.1 255.255.255.0
!
interface VLAN 103
 ip address 10.100.103.1 255.255.255.0
!
interface VLAN 104
 ip address 10.100.11.1 255.255.255.0
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.101.0 0.0.0.255 area 0
 network 10.100.102.0 0.0.0.255 area 0
 network 10.100.103.0 0.0.0.255 area 0
!
ip igmp snooping svgl vlan 104
ip igmp snooping svgl profile 1
ip igmp snooping svgl subvlan 101-103
ip igmp snooping svgl
!
```

7. Common Errors

- The multicast groups associated with the SVGL mode are not configured.
- The sent multicast traffic is not in the multicast groups associated with the SVGL mode.

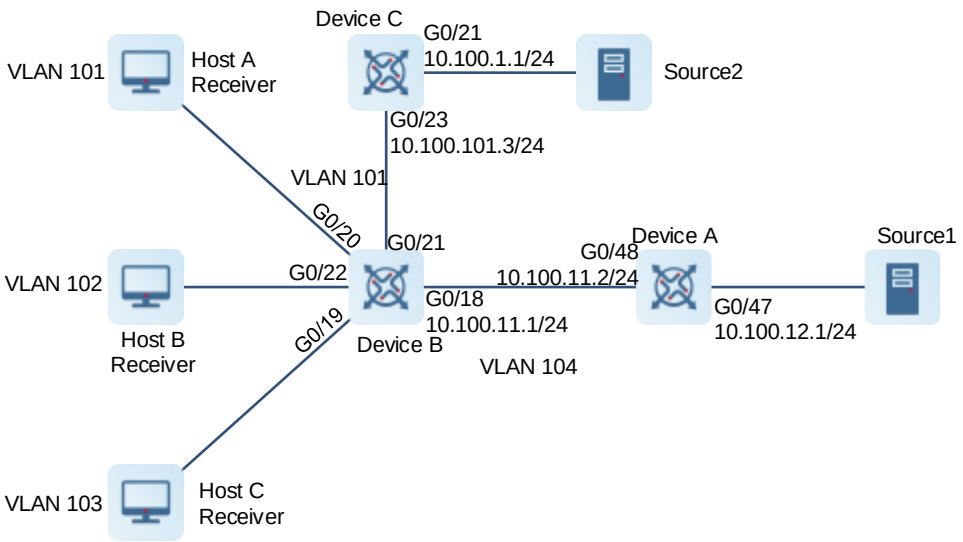
1.9.3 Configuring Basic IGMP Snooping Functions in IVGL-SVGL Mode

1. Requirements

In the multicast network shown in Figure 1-7, the routers (Device A and Device C) connect to the user network through the switch (Device B), IGMP snooping is run on Device A and Device C, and Device A and Device C directly connect to the multicast sources. Multicast source 1 sends data to multicast group 225.0.0.10, and multicast source 2 sends data to multicast group 239.0.0.11. Host A, Host B, and Host C are connected to VLAN 101, VLAN 102, and VLAN 103, respectively. Host B and Host C join multicast group 225.0.0.10, and Host A joins multicast groups 225.0.0.10 and 239.0.0.11. Host B and Host C can receive multicast data that source 1 sends to multicast group 225.0.0.10, and Host A can receive multicast data that source 1 sends to multicast group 225.0.0.10 and multicast data that source 2 sends to multicast group 239.0.0.11. Host A, Host B, and Host C enjoy shared multicast services, and Host A also enjoys independent multicast services.

2. Topology

Figure 1-7 Topology of Basic IGMP Snooping Functions in IVGL-SVGL Mode



3. Notes

Configure basic IGMP snooping functions in IVGL-SVGL mode on Device B.

- Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and PIM-SM related functions on Device A and Device C.
- Enable IGMP snooping and run the IVGL-SVGL mode on Device B.
- Configure the multicast groups associated with the IGMP snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

4. Procedure

(1) Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IP address and unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ip address 10.100.12.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# vlan 104
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ip address 10.100.11.2 255.255.255.0
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# switchport mode trunk
```

```
DeviceA(config-if-GigabitEthernet 0/48)# switchport trunk native vlan 104
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# router ospf 49
DeviceA(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceA(config-router)# network 10.100.12.0 0.0.0.255 area 0
DeviceA(config-router)# exit
```

Configure the IP address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan range 101-104
DeviceB(config-vlan-range)# exit
DeviceB(config)# interface VLAN 101
DeviceB(config-if-VLAN 101)# ip address 10.100.101.1 255.255.255.0
DeviceB(config-if-VLAN 101)# exit
DeviceB(config)# interface VLAN 102
DeviceB(config-if-VLAN 102)# ip address 10.100.102.1 255.255.255.0
DeviceB(config-if-VLAN 102)# exit
DeviceB(config)# interface VLAN 103
DeviceB(config-if-VLAN 103)# ip address 10.100.103.1 255.255.255.0
DeviceB(config-if-VLAN 103)# exit
DeviceB(config)# interface VLAN 104
DeviceB(config-if-VLAN 104)# ip address 10.100.11.1 255.255.255.0
DeviceB(config-if-VLAN 104)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/18)# switchport trunk native vlan 104
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 103
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 101
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/21
DeviceB(config-if-GigabitEthernet 0/21)# switchport access vlan 101
DeviceB(config-if-GigabitEthernet 0/21)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 102
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# router ospf 49
DeviceB(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.101.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.102.0 0.0.0.255 area 0
DeviceB(config-router)# network 10.100.103.0 0.0.0.255 area 0
DeviceB(config-router)# exit
```

Configure the IP address and unicast routing protocol on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# no switchport
DeviceC(config-if-GigabitEthernet 0/21)# ip address 10.100.1.1 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface GigabitEthernet 0/23
DeviceC(config-if-GigabitEthernet 0/23)# no switchport
DeviceC(config-if-GigabitEthernet 0/23)# ip address 10.100.101.3 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/23)# exit
DeviceC(config)# router ospf 49
DeviceC(config-router)# network 10.100.1.0 0.0.0.255 area 0
DeviceC(config-router)# network 10.100.101.0 0.0.0.255 area 0
DeviceC(config-router)# exit
```

(2) Enable multicast routing and PIM-SM related functions on Device A and Device C.

Enable multicast routing and PIM-SM related functions on Device A.

```
DeviceA(config)# ip multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ip pim sparse-mode
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# ip pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ip pim rp-candidate GigabitEthernet 0/47
```

Enable multicast routing and PIM-SM related functions on Device C.

```
DeviceC(config)# ip multicast-routing
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# no switchport
DeviceC(config-if-GigabitEthernet 0/21)# ip pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface GigabitEthernet 0/23
DeviceC(config-if-GigabitEthernet 0/23)# ip pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/23)# exit
```

(3) Enable IGMP snooping and run the IVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping ivgl-svgl
```

(4) Configure the multicast groups associated with the IGMP snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp profile 1
DeviceB(config-profile)# permit
```

```
DeviceB(config-profile)# range 224.1.1.1 238.1.1.1
DeviceB(config-profile)# exit
DeviceB(config)# ip igmp snooping svgl profile 1
DeviceB(config)# ip igmp snooping svgl vlan 104
DeviceB(config)# ip igmp snooping svgl subvlan 101-103
```

5. Verification

Run the **show ip igmp snooping gda-table** command on Device B to display the IGMP snooping forwarding entries and check whether the member port list of entry (*, 225.0.0.10, 104) contains GigabitEthernet 0/22, GigabitEthernet 0/20, and GigabitEthernet 0/19 and the member port list of entry (*, 239.0.0.11, 101) contains GigabitEthernet 0/20.

```
DeviceB> enable

DeviceB# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 239.0.0.11, 101):
  VLAN(101) 2 OPORTS:
    GigabitEthernet 0/20(D)
    GigabitEthernet 0/21(M)

(*, 225.0.0.10, 104):
  VLAN(104) 1 OPORTS:
    GigabitEthernet 0/18(M)

  VLAN(102) 1 OPORTS:
    GigabitEthernet 0/22(D)

  VLAN(101) 1 OPORTS:
    GigabitEthernet 0/20(D)

  VLAN(103) 1 OPORTS:
    GigabitEthernet 0/19(D)

DeviceB#
```

Run the **show ip igmp snooping** command on Device B and check whether the IGMP snooping working mode is IVGL-SVGL.

```
DeviceB# show ip igmp snooping
IGMP Snooping running mode: IVGL-SVGL
IGMP Snooping L2-entry-limit: 64000
SVGL vlan: 104
SVGL profile number: 1
IGMP Snooping SVGL subvlan: 101-103
```

```
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Global Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Snooping version: 2
IGMP Preview group aging time: 60(Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)

vlan 1
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC

vlan 101
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC

vlan 102
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC

vlan 103
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC

vlan 104
-------------
```

```
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Enabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip multicast-routing
!
vlan 104
!
interface GigabitEthernet 0/47
 no switchport
 ip address 10.100.12.1 255.255.255.0
ip pim sparse-mode
!
interface GigabitEthernet 0/48
 switchport mode trunk
 switchport trunk native vlan 104
!
interface VLAN 104
 ip address 10.100.11.2 255.255.255.0
ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.12.0 0.0.0.255 area 0
!
ip pim bsr-candidate GigabitEthernet 0/48
ip pim rp-candidate GigabitEthernet 0/48
!
```

- Device B configuration file

```
hostname DeviceB
!
ip igmp profile 1
 permit
 range 224.1.1.1 238.1.1.1
!
vlan range 1,101-104
!
```

```
interface GigabitEthernet 0/18
 switchport mode trunk
 switchport trunk native vlan 104
!
interface GigabitEthernet 0/19
 switchport access vlan 103
!
interface GigabitEthernet 0/20
 switchport access vlan 101
!
interface GigabitEthernet 0/21
 switchport access vlan 101
!
interface GigabitEthernet 0/22
 switchport access vlan 102
!
interface VLAN 101
 ip address 10.100.101.1 255.255.255.0
!
interface VLAN 102
 ip address 10.100.102.1 255.255.255.0
!
interface VLAN 103
 ip address 10.100.103.1 255.255.255.0
!
interface VLAN 104
 ip address 10.100.11.1 255.255.255.0
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.101.0 0.0.0.255 area 0
 network 10.100.102.0 0.0.0.255 area 0
 network 10.100.103.0 0.0.0.255 area 0
!
ip igmp snooping svgl vlan 104
ip igmp snooping svgl profile 1
ip igmp snooping svgl subvlan 101-103
ip igmp snooping ivgl-svgl
!
```

- Device C configuration file

```
hostname DeviceC
!
ip multicast-routing
!
interface GigabitEthernet 0/21
```

```
 no switchport
 ip address 10.100.1.1 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet 0/23
 no switchport
 ip address 10.100.101.3 255.255.255.0
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.1.0 0.0.0.255 area 0
 network 10.100.101.0 0.0.0.255 area 0
!
```

7. Common Errors

- The multicast groups associated with the SVGL mode are not configured.
- The sent multicast traffic is not in the multicast groups associated with the SVGL mode.
- The group addresses of multicast traffic in IVGL mode are within the multicast group range in SVGL mode. As a result, IVGL forwarding cannot be implemented.

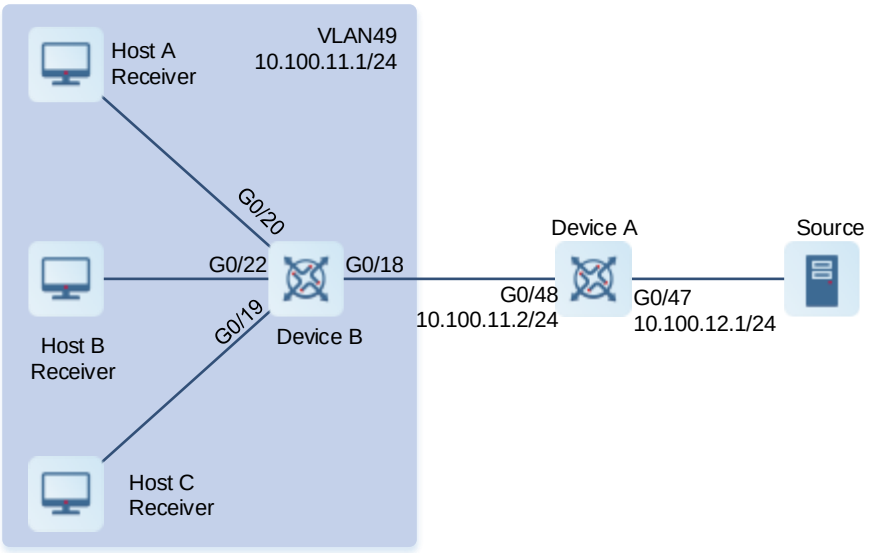
1.9.4 Configuring Static Ports to Implement L2 Multicast

1. Requirements

In the multicast network shown in Figure 1-8, Host A, Host B, and Host C need to receive data that a multicast source sends to a specific multicast group stably. The router (Device A) connects to the user network through the L2 device (Device B). The static IGMP multicast groups 225.0.0.10 to 225.0.0.12 are configured on the user-side L3 port on Device A. Host A and Host B want to receive data of multicast group 225.0.0.10 stably, and Host C wants to receive data of multicast group 225.0.0.11 stably.

2. Topology

Figure 1-8 Topology of Static Ports to Implement L2 Multicast



3. Notes

Configure IGMP snooping static multicast router ports and member ports on Device B.

- Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and IGMP static multicast groups on Device A.
- Enable IGMP snooping on Device B.
- Configure static multicast router ports and member ports on Device B.

4. Procedure

(1) Configure the IP addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IP address and unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ip address 10.100.12.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# no switchport
DeviceA(config-if-GigabitEthernet 0/48)# ip address 10.100.11.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# router ospf 49
DeviceA(config-router)# network 10.100.11.0 0.0.0.255 area 0
```

```
DeviceA(config-router)# network 10.100.12.0 0.0.0.255 area 0
DeviceA(config-router)# exit
```

Configure the IP address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan 49
DeviceB(config-vlan)# exit
DeviceB(config)# interface vlan 49
DeviceB(config-if-VLAN 49)#ip address 10.100.11.1 255.255.255.0
DeviceB(config-if-VLAN 49)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# router ospf 49
DeviceB(config-router)# network 10.100.11.0 0.0.0.255 area 0
DeviceB(config-router)# exit
```

(2) Enable IP multicast routing and PIM-SM related functions on Device A.

```
DeviceA(config)# ip multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# ip igmp static-group 225.0.0.10
DeviceA(config-if-GigabitEthernet 0/48)# ip igmp static-group 225.0.0.11
DeviceA(config-if-GigabitEthernet 0/48)# ip igmp static-group 225.0.0.12
DeviceA(config-if-GigabitEthernet 0/48)# ip pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ip pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ip pim rp-candidate GigabitEthernet 0/47
```

(3) Enable basic IGMP snooping functions on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping ivgl
```

(4) Configure static multicast router ports and member ports on Device B.

```
DeviceB> enable
```

```
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping vlan 49 static 225.0.0.11 interface
GigabitEthernet 0/19
DeviceB(config)# ip igmp snooping vlan 49 static 225.0.0.10 interface
GigabitEthernet 0/22
DeviceB(config)# ip igmp snooping vlan 49 static 225.0.0.10 interface
GigabitEthernet 0/20
DeviceB(config)# ip igmp snooping vlan 49 mrouter interface GigabitEthernet 0/18
```

5. Verification

Run the **show ip igmp snooping mrouter** command and check whether the static router port is GigabitEthernet 0/18.

```
DeviceB> enable
DeviceB# show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 49):
  VLAN(49)  1 MROUTES:
    GigabitEthernet 0/18(DS)

(*, *, 101):
  VLAN(101)  1 MROUTES:
    GigabitEthernet 0/21(D)

DeviceB#
```

Run the **show ip igmp snooping gda-table** command and check whether the static member ports of multicast group 225.0.0.10 are GigabitEthernet 0/20 and GigabitEthernet 0/22 and the static member port of multicast group 225.0.0.11 is GigabitEthernet 0/19.

```
DeviceB# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 225.0.0.10, 49):
  VLAN(49) 3 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/20(S)
    GigabitEthernet 0/22(S)

(*, 225.0.0.11, 49):
  VLAN(49) 2 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/19(S)
```

```
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip multicast-routing
!
interface GigabitEthernet 0/47
 no switchport
 ip address 10.100.12.1 255.255.255.0
ip pim sparse-mode
!
interface GigabitEthernet 0/48
 no switchport
 ip address 10.100.11.2 255.255.255.0
 ip igmp static-group 225.0.0.10
 ip igmp static-group 225.0.0.11
 ip igmp static-group 225.0.0.12
 ip pim sparse-mode
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
 network 10.100.12.0 0.0.0.255 area 0
!
ip pim bsr-candidate GigabitEthernet 0/47
ip pim rp-candidate GigabitEthernet 0/47
!
```

- Device B configuration file

```
hostname DeviceB
!
vlan range 1,49
!
interface GigabitEthernet 0/18
 switchport access vlan 49
!
interface GigabitEthernet 0/19
 switchport access vlan 49
!
interface GigabitEthernet 0/20
 switchport access vlan 49
!
interface GigabitEthernet 0/22
 switchport access vlan 49
```

```
!
interface VLAN 49
 ip address 10.100.11.1 255.255.255.0
!
router ospf 49
 graceful-restart
 network 10.100.11.0 0.0.0.255 area 0
!
ip igmp snooping ivgl
!
ip igmp snooping vlan 49 static 225.0.0.11 interface GigabitEthernet 0/19
ip igmp snooping vlan 49 static 225.0.0.10 interface GigabitEthernet 0/22
ip igmp snooping vlan 49 static 225.0.0.10 interface GigabitEthernet 0/20
ip igmp snooping vlan 49 mrouter interface GigabitEthernet 0/18
!
```

7. Common Errors

- Basic IGMP snooping functions are not configured or fail to be configured.

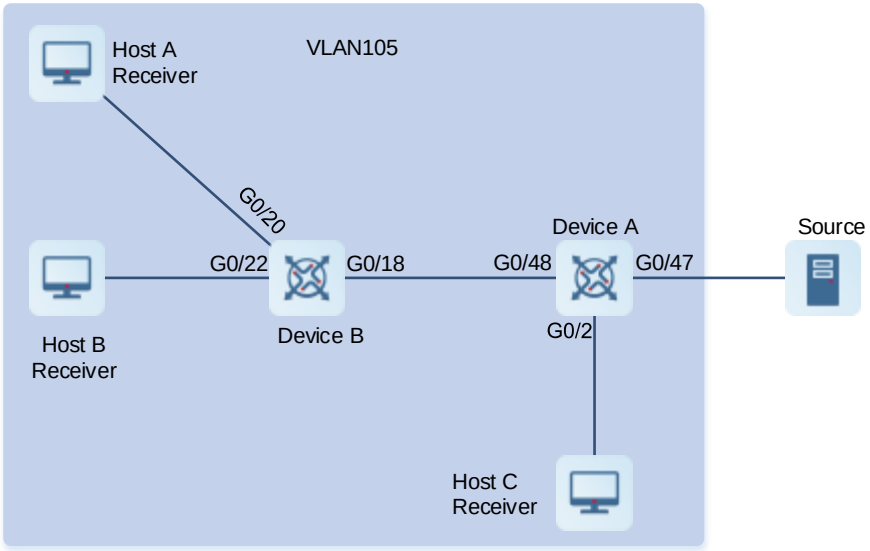
1.9.5 Configuring IGMP Snooping Querier

1. Requirements

In a two-layer multicast network, as shown in Figure 1-9, the multicast source sends multicast data to multicast groups 225.0.0.10 and 225.0.0.11. Host A and Host C join multicast group 225.0.0.10, and Host B joins multicast group 225.0.0.11. All receivers use IGMPv2. IGMP snooping is used to transfer multicast data in the two-layer network.

2. Topology

Figure 1-9 Topology of IGMP Snooping Querier



3. Notes

Enable IGMP snooping on Device A and Device B, and configure Device A as the IGMP snooping querier.

- Configure VLANs and IP addresses on Device A and Device B.
- Enable IGMP snooping and run the IVGL mode on Device A and Device B.
- Configure the IGMP snooping querier function for VLAN 105 on Device A.

4. Procedure

(1) Configure VLANs and IP addresses on Device A and Device B.

Configure the VLAN and IP address on Device A.

```
DeviceA>enable
DeviceA# configure terminal
DeviceA(config)# vlan range 1,105
DeviceA(config)# interface VLAN105
DeviceA(config-if-VLAN105)# ip address 10.100.12.1 255.255.255.0
DeviceA(config-if-VLAN105)# exit
DeviceA(config)# interface GigabitEthernet0/47
DeviceA(config-if-GigabitEthernet0/47)# switchport access vlan 105
DeviceA(config-if-GigabitEthernet0/47)# interface GigabitEthernet0/48
DeviceA(config-if-GigabitEthernet0/48)# switchport mode trunk
DeviceA(config-if-GigabitEthernet0/48)# switchport trunk native vlan 105
DeviceA(config-if-GigabitEthernet0/48)# exit
```

Configure the VLAN and IP address on Device B.

```
DeviceB>enable
DeviceB# configure terminal
DeviceB(config)# vlan range 1,105
DeviceB(config)# interface VLAN105
DeviceB(config-if-VLAN105)# ip address 10.100.12.3 255.255.255.0
DeviceB(config-if-VLAN105)# exit
DeviceB(config-if-GigabitEthernet 0/18)# interface GigabitEthernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/2)# exit
DeviceB(config)#interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/18)# switchport trunk native vlan 105
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 105
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 105
DeviceB(config-if-GigabitEthernet 0/22)# exit
```

(2) Configure basic IGMP snooping functions and run the IVGL mode on Device A and Device B.

Enable IGMP snooping and run the IVGL mode on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip igmp snooping ivgl
```

Enable IGMP snooping and run the IVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip igmp snooping ivgl
```

(3) Configure the IGMP snooping querier function on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)#ip igmp snooping querier
DeviceA(config)#ip igmp snooping querier address 10.100.12.1
DeviceA(config)#ip igmp snooping vlan 105 querier
```

5. Verification

Run the **show ip igmp snooping querier** command to check whether the querier of VLAN 1 takes effect.

```
DeviceA> enable
DeviceA# show ip igmp snooping querier
Vlan     IP Address         IGMP Version         Port
-----------------------------------------------------------
105      10.100.12.1            2                switch
DeviceA#
DeviceA# show ip igmp snooping querier vlan 105

Vlan 105:   IGMP switch querier status
-------------------------------------------------------
elected querier is 10.100.12.1        (this switch querier)
-------------------------------------------------------
admin state                 : Enable
admin version               : 2
source IP address            : 10.100.12.1
query-interval (sec)         : 60
max-response-time (sec)       : 10
querier-timeout (sec)        : 125
operational state            : Querier
operational version          : 2
DeviceA#
```

Run the **show ip igmp snooping gda-table** command on Device A and check whether the outbound ports of multicast group 225.0.0.10 are GigabitEthernet0/2 and GigabitEthernet0/48 and the outbound port of multicast group 225.0.0.11 is GigabitEthernet0/48.

```
DeviceA> enable
DeviceA# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
```

```
  S: STATIC
  M: MROUTE
(*, 225.0.0.10, 105):
  VLAN(105) 2 OPORTS:
    GigabitEthernet0/2(D)
    GigabitEthernet0/48(D)

(*, 225.0.0.11, 105):
  VLAN(105) 1 OPORTS:
    GigabitEthernet0/48(D)

DeviceA#
```

Run the **show ip igmp snooping gda-table** command on Device B and check whether the outbound port of multicast group 225.0.0.10 is GigabitEthernet0/20 and the outbound port of multicast group 225.0.0.11 is GigabitEthernet0/22.

```
DeviceB> enable
DeviceB# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 225.0.0.10, 105):
  VLAN(105) 2 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/20(D)

(*, 225.0.0.11, 105):
  VLAN(105) 2 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/22(D)

DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
vlan range 1,105
!
interface GigabitEthernet0/2
 switchport access vlan 105
!
interface GigabitEthernet0/47
 switchport access vlan 105
!
```

```
interface GigabitEthernet0/48
 switchport mode trunk
 switchport trunk native vlan 105
!
interface VLAN105
 ip address 10.100.12.1 255.255.255.0
!
ip igmp snooping ivgl
ip igmp snooping querier
ip igmp snooping querier address 10.100.12.1
ip igmp snooping vlan 105 querier
!
```

- Device B configuration file

```
hostname DeviceA
!
vlan range 1,105
!
interface GigabitEthernet 0/18
 switchport mode trunk
 switchport trunk native vlan 105
!
interface GigabitEthernet 0/20
 description cyx
 switchport access vlan 105
!
interface GigabitEthernet 0/22
 description cyx
 switchport access vlan 105
!
interface VLAN 105
 ip address 10.100.12.3 255.255.255.0
!
ip igmp snooping ivgl
!
```

7. Common Errors

- The source IP address of Query packets sent by the querier is not configured. As a result, the querier function does not take effect.

Contents

1 Configuring MSDP 1
1.1 Introduction 1
1.1.1 Principles 1
1.1.2 Protocols and Standards 8
1.2 Restrictions and Guidelines 8
1.3 Configuration Task Summary 8
1.4 Prerequisites 9
1.5 Managing MSDP Peers 9
1.5.1 Overview 9
1.5.2 Configuration Tasks 9
1.5.3 Configuring MSDP Peers 10
1.5.4 Configuring the Default MSDP Peer 10
1.5.5 Configuring an MSDP Mesh Group 11
1.5.6 Configuring the TCP Reconnection Interval of an MSDP Peer 11
1.5.7 Enabling MD5 Authentication on TCP Connections Between MSDP Peers 12
1.5.8 Configuring the Number of MSDP Peers Supported on a Device 12
1.6 Restricting SA Messages 13
1.6.1 Overview 13
1.6.2 Configuration Tasks 13
1.6.3 Prerequisites 13
1.6.4 Configuring the TTL Value of Multicast Packets in SA Messages 13
1.6.5 Enabling the Function of Filtering Source Information Released Locally 14

1.6.6 Enabling the Function of Filtering Received SA Requests 14

1.6.7 Enabling the Function of Filtering Received SA Messages 15

1.6.8 Enabling the Function of Filtering Sent SA Messages 16

1.6.9 Configuring SA Cache Capacity 16

1.7 Configuring an Anycast RP 17

1.7.1 Overview 17

1.7.2 Prerequisites 17

1.7.3 Procedure 17

1.8 Monitoring 18

1.9 Configuration Examples 19

1.9.1 Enabling Basic Functions of MSDP 19

1.9.2 Configuring an Anycast RP 24

1.9.3 Enabling MD5 Authentication 30

1.9.4 Managing MSDP Peers 33

1.9.5 Modifying Protocol Parameters 35

1 Configuring MSDP

1.1 Introduction

Multicast Source Discovery Protocol (MSDP) is used to connect multiple rendezvous points (RPs) on the multicast network and implement the following two functions.

- Use MSDP among multiple Protocol Independent Multicast Sparse-Mode (PIM-SM) domains to share the multicast source information of these PIM-SM domains to implement cross-domain multicast.

  With the increase of a network, a PIM network can be divided into multiple PIM-SM domains to facilitate management. The RPs in a domain cannot understand multicast source information in other domains. MSDP peers are created among the PIM-SM domains to interact source-active (SA) messages so that multicast source information can be shared and multicast packets can be forwarded to hosts in other domains.

- Use MSDP in a PIM-SM domain to share the multicast source information of multiple RPs to implement an anycast RP.

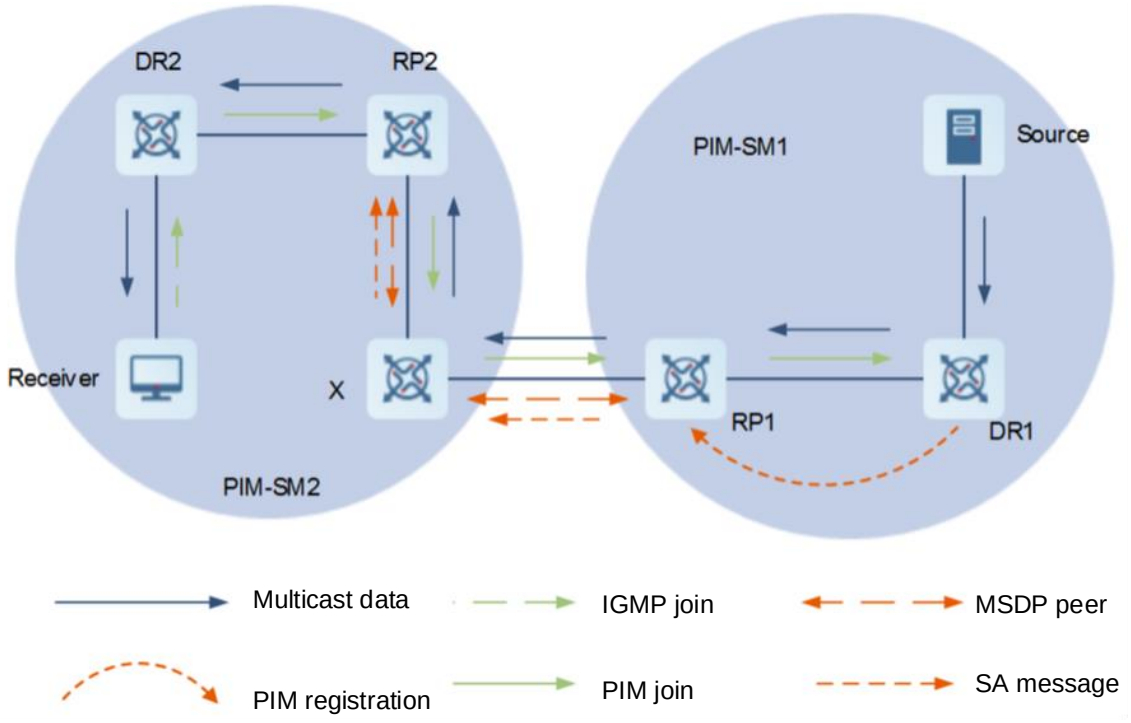
  After RPs in a PIM-SM domain are configured with the same address and MSDP peers are created on these RPs, the RPs can implement load sharing and backup in the PIM-SM domain.

1.1.1 Principles

1. MSDP Peer

Configure one or more pairs of MSDP peers on the network to connect RPs. The peers interact SA messages so that an RP can notify other RPs of the multicast source information on this RP. So far as the unicast route is reachable, the MSDP peer relationship can be established. MSDP peers can be configured on RPs as well as on any other PIM device, for example, X in Figure 1-1.

Figure 1-1 Positions of MSDP Peers



- RP connected to the multicast source

  Configure the MSDP peer on the RP connected to the multicast source. Then, this RP can use SA messages to send the local multicast source information to other RPs.

  As shown in Figure 1-1, DR 1 registers the multicast source information with RP 1. As a peer relationship is established between RP 1 and the PIM device X, RP 1 sends the multicast source information to the PIM device X.

- SA message forwarder

  Non-RPs (common PIM devices) can also act as MSDP peers, but only forward SA messages.

  As shown in Figure 1-1, X forwards SA messages sent from RP 1 to RP 2. In this way, the multicast source information is transferred to RP 2.

- RP connected to the multicast receiver

  Configure the MSDP peer on the RP connected to the multicast receiver. Then, this RP can trigger a join towards the multicast source based on the received SA message.

  As shown in Figure 1-1, DR 2 triggers a join towards RP 2. As RP 2 already obtains the multicast source information, RP 2 continues to trigger a join towards the multicast source, thus establishing a multicast distribution tree (MDT) from DR 1 to DR 2.

2. MSDP Packet

An MSDP packet is encapsulated in a TCP packet and follows the format of type-length-value (TLV), as shown in Figure 1-2.

Figure 1-2 Format of MSDP Packet

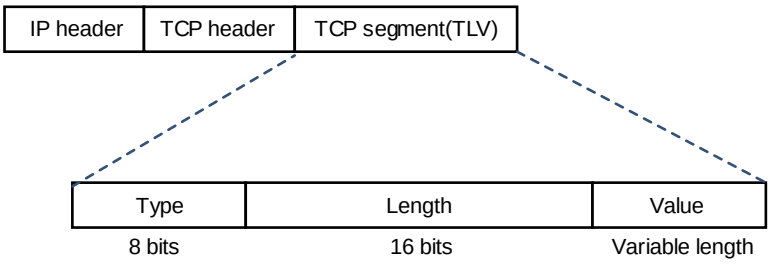


Table 1-1 Fields of MSDP Packet

Field	Length	Description
Type	8 bits	Specifies a message type. ● **1**: Source-Active. Messages of this type carry multiple pairs of (S, G) information and they are transmitted among RPs. PIM-SM multicast packets can be encapsulated in the messages. ● **2**: Source-Active Request. Messages of this type request an (S, G) list of a specified group G to reduce the source join delay. ● **3**: Source-Active Response. Messages of this type are responses to the Source-Active Request. ● **4**: Keep Alive. Messages of this type hold the connection relationship of MSDP peers. ● **5**: Reserved. This is the reserved type of messages. ● **6**: MSDP traceroute in progress. Messages of this type specify the Traceroute function of MSDP and detect the reverse path forwarding (RPF) of SA messages. ● **7**: MSDP traceroute reply. Messages of this type specify the Traceroute function of MSDP and detect the RPF of SA messages.
Length	16 bits	Specifies the length of a message in bytes. The length includes the Type, Length and Value fields. Except for the Keep Alive message, the length of other messages must be 4 bytes at least and 9192 bytes at most.
Value	Subject to the length of the variable	Specifies the message content, which varies with the message type.

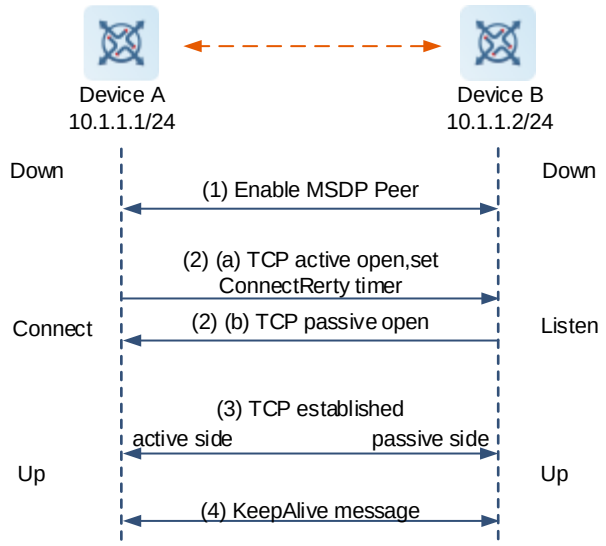
Based on Table 1-1, SA messages can carry multiple pairs of (S, G) information and they are transmitted among RPs. PIM-SM multicast packets can be encapsulated in the messages. The peers interact SA messages with each other to share multicast source information. Multicast packets are encapsulated in the SA messages to avoid the (S, G) entries in the SA messages timeout. If this is the case, hosts cannot receive the multicast packets of the source.

MSDP supports periodic sending of SA requests and SA responses to improve the source information update efficiency. With the mechanism, new hosts do not need to wait for an SA sending period to obtain valid (S, G) information, which reduces the time for the hosts to join a shortest path tree (SPT).

3. MSDP Peer Establishment Procedure

MSDP peers are connected over TCP through port 639. After a TCP connection is established between the peers, the connection is maintained through the keep alive messages.

Figure 1-3 MSDP Peer Connection Establishment Procedure



As shown in Figure 1-3, initially, the MSDP session state of device A and device B is down. The MSDP peer connection establishment procedure is as follows:

(1) Device A and device B specify the other party as a peer mutually and they compare their addresses.

  a The IP address of device A is smaller than that of device B. Therefore, device A enters the connection status, initiates a connection request to device B, and starts a timer for reconnection.

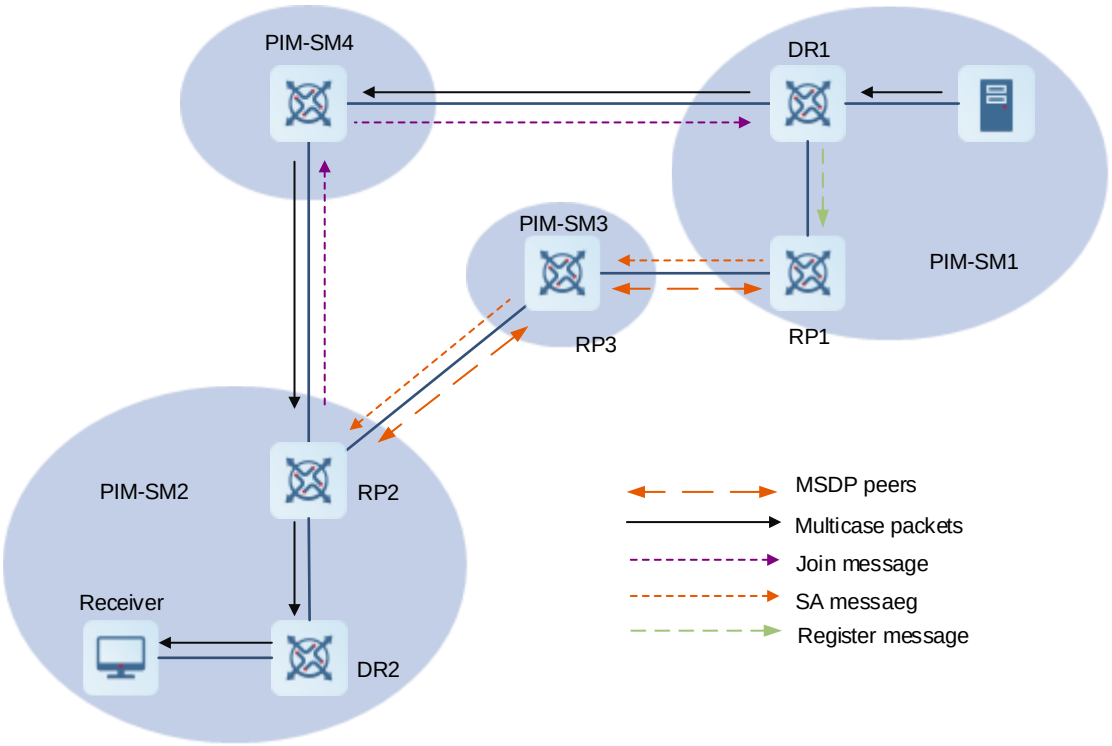
  b The IP address of device B is greater. Therefore, device B enters the listening status and waits for the connection request.

(2) After the MSDP session is established between device A and device B, the connection status is up. The two devices send keep alive messages to each other to notify the other party of keeping the MSDP session.

4. Inter-domain Multicast of MSDP

As shown in Figure 1-4, the multicast network is divided into four PIM-SM domains. In PIM-SM 1, the active source sends multicast data to the multicast group and registers with RP 1. In PIM-SM 2, the receiver joins the group, expecting to receive multicast data from the source in PIM-SM 1. The devices in PIM-SM 2 and PIM-SM 3 need to know the position of the source so as to obtain the corresponding multicast data. To implement this purpose, MSDP peer relationship must be established between RP 1 and RP 3 and between RP 3 and RP 2.

Figure 1-4 Inter-domain Multicast of MSDP



The working process of PIM-SM inter-domain multicast is as follows:

(1) The multicast source in PIM-SM 1 sends multicast data to the group. The multicast data is sent to source DR 1 for registration and encapsulated in messages and sent to RP 1. RP 1 obtains the multicast source information.

(2) Source RP 1 sends SA messages to RP 3 periodically. An SA message contains the multicast source address S, multicast group address G, and RP 1 address.

(3) Upon receiving the SA messages, RP 3 performs RPF checking and filters forwarding policies. After the messages pass the checking, they are sent to RP 2. Then, PIM-SM 2 and PIM-SM 3 obtain the source information.

(4) Upon receiving the SA messages, RP 2 checks whether the receiver of the group exists in PIM-SM 2.

- If the receiver exists in PIM-SM 2, an RPT about the group is created between RP 2 and the receiver. RP 2 creates an (S, G) pair and sends an (S, G) join packet to the source hop by hop to generate an SPT. The multicast data is sent to RP 2 along the SPT and then forwarded to the receiver along the RPT. Upon receiving the multicast data, member DR 2 decides whether to perform SPT switchover based on configuration.
- If the receiver does not exist in PIM-SM 2, RP 2 does not create an (S, G) pair or send join packets to the source.

5. Receiving and Forwarding SA Messages

An SA message contains the multicast source address, multicast group address, and RP address. The RP address is the IP address of the RP with which the multicast source is registered.

- The RP encapsulates the locally registered multicast source information in an SA message, and sends the

message to all its MSDP peers.

- On receiving the SA message, each MSDP peer performs the peer RPF check, compares the SA message with the content in the SA cache, and matches the SA message against the SA incoming and outgoing filtering rules. If the SA message passes the peer RPF check and meets the outgoing filtering rules and does not exist in the SA cache, this SA message is forwarded to other MSDP peers.
- For any SA message coming from an MSDP peer (address: N), the following peer RPF check rules are used to prevent loops and avoid SA message flooding:

  a If N is a member of the mesh group, the SA message passes the peer RPF check; otherwise, go to step b.

  b If N is the only active MSDP peer on the local device, the SA message passes the peer RPF check; otherwise, go to step c.

  c If N is the RP address in the SA message, the SA message passes the peer RPF check; otherwise, go to step d.

  d If an EBGP route to the RP address in the SA message exists on the local device and the next hop of this route is N, the SA message passes the peer RPF check; otherwise, go to step e.

  e If an optimum route to the RP address in the SA message exists on the local device, check as follows:

  If this optimum route is a distance vector route (such as the BGP/RIP route), and this router is advertised by N, the SA message passes the peer RPF check.

  If this optimum route is a link status route (such as the OSPF/IS-IS route), and the next hop of this router is N, the SA message passes the peer RPF check.

  Otherwise, go to step f.

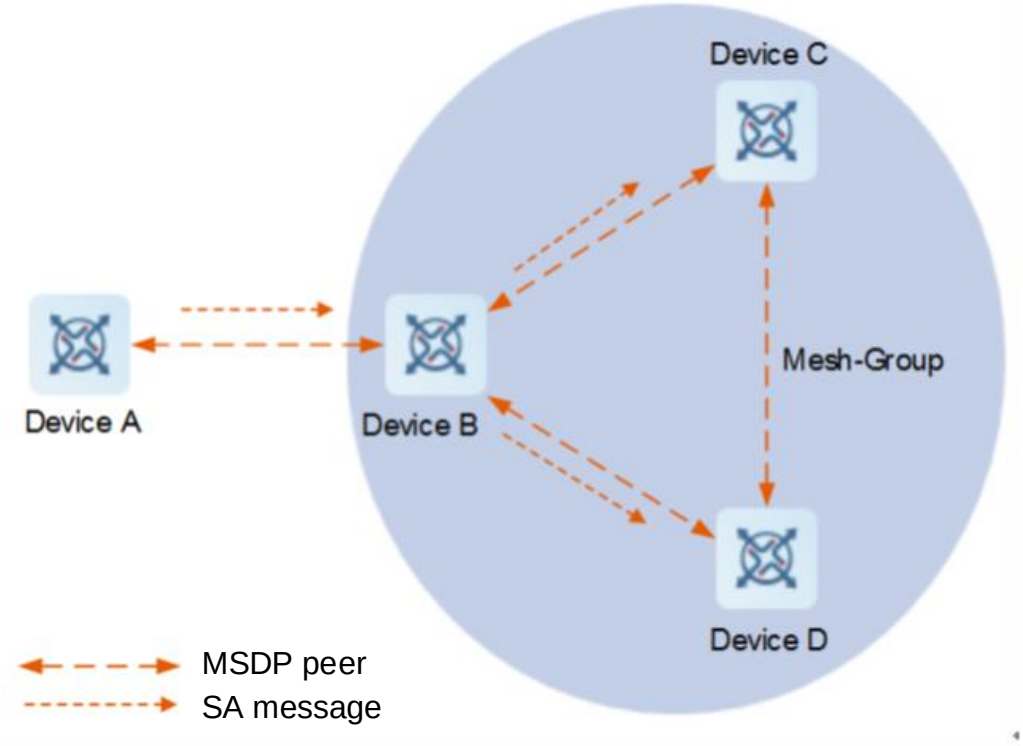
  f If an optimum route to the RP address in the SA message exists on the local device, and this route is an MBGP/BGP route, extract the nearest autonomous system (AS) of the AS path of this MBGP/BGP route. If the local device has multiple MSDP peers in this AS and N is the MSDP peer with the largest IP address, or N is the only MSDP peer in this AS, the SA message passes the peer RPF check; otherwise, go to step g.

  g If N is the default MSDP peer, the SA message passes the peer RPF check; otherwise, go to step h.

  h The SA message fails in the peer RPF check.

- When MSDP peer relationship is established on any two members in a group, this group is a mesh group. The mesh group helps reduce the number of SA messages. As shown in Figure 1-5, device B, device C, and device D belong to the same mesh group.
  - For SA messages from device A outside the mesh group and received by device B in the mesh group, after the messages pass the peer RPF check and SA cache comparison, these SA messages are forwarded to other members in the group.
  - For SA messages from device B to device C and device D, they are no longer forwarded to other members in the group.

Figure 1-5 Mesh Group Topology



- The SA cache buffers status of SA messages. Expired SA messages will be deleted.
  - When an MSDP peer receives an SA message

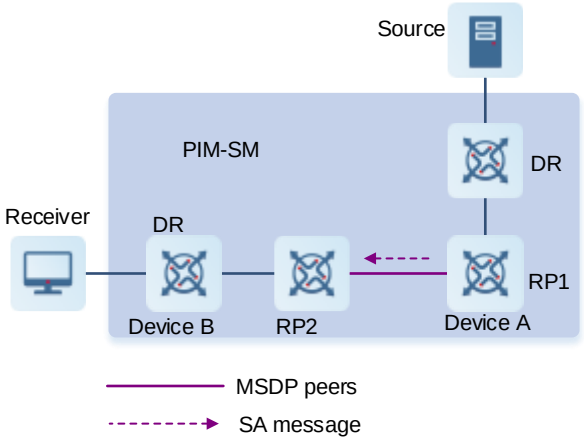
    If this message does not exist in the SA cache and passes the peer RPF check, the message is stored in the SA cache.

    If this message already exists in the SA cache, the message is ignored. This helps suppress SA message flooding.
  - When an MSDP peer receives an SA message, if this message already exists in the SA cache, the message is immediately responded. This helps improve the protocol efficiency.

6. Anycast RP based on MSDP

Generally, each multicast group in a PIM-SM network is served by only one RP. If the RP is faulty or fails, the multicast traffic may be interrupted. Anycast RP enables multiple RPs with the same address to serve a multicast group to implement redundant backup between the RPs. The multicast sources or group members register with the nearest RPs so that the RPs synchronize source information. Anycast RP is implemented by creating MSDP peer relationship between these RPs.

Figure 1-6 Anycast RP based on MSDP



As shown in Figure 1-6, device A and device B in a PIM-SM domain establish peer relationship. The source sends multicast data to the group, and the receiver receives the multicast data as a member of the group. The working process of Anycast RP based on MSDP is as follows:

(1) When the source DR receives the multicast data from the source, the source DR registers with the nearest RP 1.

(2) When the member DR receives a join request packet from the receiver, the member DR forwards the join packet to RP 2. In this way, an RPT with RP 2 as the root is formed.

(3) RP 1 and RP 2 interact SA messages and share the (S, G) information of the multicast source. Upon obtaining the multicast source information, RP 2 sends the join packet to the source hop by hop to generate an SPT.

(4) The multicast data is forwarded to RP 2 through the SPT and then forwarded to the receiver through the RPT. The member DR decides whether to perform SPT switchover based on configuration.

1.1.2 Protocols and Standards

- RFC3618: Multicast Source Discovery Protocol (MSDP)
- RFC 3446: Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

1.2 Restrictions and Guidelines

Establish the MSDP peer relationship between multiple ASs so that group members can apply for the multicast streams across ASs.

- The inter-AS unicast route must be reachable.
- Run PIM-SM within each AS, and configure the BSR border.
- The IP address and local interface of the MSDP peer must be the same as those of the EBGP peer.

1.3 Configuration Task Summary

The IP multicast configuration includes the following tasks:

(1) Managing MSDP Peers.

- Configuring MSDP Peers
- (Optional) Configuring the Default MSDP Peer
- (Optional) Configuring an MSDP Mesh Group
- (Optional) Configuring the TCP Reconnection Interval of an MSDP Peer
- (Optional) Enabling MD5 Authentication on TCP Connections Between MSDP Peers
- (Optional) Configuring the Number of MSDP Peers Supported on a Device

(2) Restricting SA Messages. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the TTL Value of Multicast Packets in SA Messages
- Enabling the Function of Filtering Source Information Released Locally
- Enabling the Function of Filtering Received SA Requests
- Enabling the Function of Filtering Received SA Messages
- Enabling the Function of Filtering Sent SA Messages
- Configuring SA Cache Capacity

(3) Configuring an Anycast RP.

1.4 Prerequisites

- Unicast routing protocols are configured and the network in a domain is reachable.
- Basic PIM-SM functions are configured to implement multicast in a domain.

1.5 Managing MSDP Peers

1.5.1 Overview

MSDP peers in different PIM-SM domains interact SA messages to share inter-domain multicast source information.

1.5.2 Configuration Tasks

The MSDP peer management configuration includes the following tasks:

(1) Configuring MSDP Peers

(2) (Optional) Configuring the Default MSDP Peer

(3) (Optional) Configuring an MSDP Mesh Group

(4) (Optional) Configuring the TCP Reconnection Interval of an MSDP Peer

(5) (Optional) Enabling MD5 Authentication on TCP Connections Between MSDP Peers

(6) (Optional) Configuring the Number of MSDP Peers Supported on a Device

1.5.3 Configuring MSDP Peers

1. Overview

MSDP peers are identified based on addresses. The relationship between MSDP peers is bidirectional. Therefore, they must be created on both ends. You can manage MSDP peers by adding description information to a specified MSDP. A connection with a specified peer can be temporarily disabled by configuration.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Establish an MSDP peer relationship.

ip msdp peer *ipv4-peer-address* **connect-source** *interface-type interface-number*

No MSDP peer is added by default.

(4) (Optional) Configure description information for an MSDP peer.

ip msdp description *ipv4-peer-address description*

No description information is added for an MSDP peer by default.

(5) (Optional) Disable an MSDP peer.

ip msdp shutdown *ipv4-peer-address*

The connection with an MSDP peer is enabled by default.

Only the TCP connection with the MSDP peer is disabled, and this MSDP peer and the configuration of this MSDP peer are reserved.

1.5.4 Configuring the Default MSDP Peer

1. Overview

On an MSDP peer, if it is not necessary to perform peer RPF check on SA messages sent from a specified peer, configure this peer as the default peer.

2. Restrictions and Guidelines

- If the **prefix-list** keyword parameter is not specified, all SA messages are accepted.
- If an inexistent **prefix-list** is specified, all SA messages are accepted.
- If an existent **prefix-list** is specified, only the SA messages of RPs specified in this prefix list are accepted.

3. Prerequisites

- An MSDP peer relationship is established.
- If the **prefix-list** keyword parameter is specified, the prefix list must be created before a default MSDP peer is configured. For details about the prefix list configuration, see *Configuring Routing Policies*.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a default MSDP peer.

ip msdp default-peer *ipv4-peer-address* [**prefix-list** *prefix-list-name*]

No default MSDP peer is configured by default.

1.5.5 Configuring an MSDP Mesh Group

1. Overview

When MSDP peer relationship is established on any two members in a group, this group is a mesh group. The mesh group helps reduce the number of SA messages and avoids SA message flooding between the peers. SA messages received by peers in a mesh group are processed in one of the following ways:

- For SA messages coming outside the mesh group, after the SA messages pass the peer RPF check and SA cache comparison, they are forwarded to the other members in the group.
- For SA messages from the internal mesh group, they are received without passing peer RPF check and are no longer forwarded to the other members in the group.

2. Restrictions and Guidelines

Among multiple MSDP peers, if SA messages from these peers pass RPF check by default, these peers can be added to a mesh group.

3. Prerequisites

An MSDP peer relationship is established.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a mesh group.

ip msdp mesh-group *mesh-name ipv4-peer-address*

No mesh group is configured and no MSDP peer is added to any mesh group by default.

1.5.6 Configuring the TCP Reconnection Interval of an MSDP Peer

1. Overview

Within the TCP reconnection interval, the MSDP peer on the proactive connection side can initiate at most one TCP connection. In some application scenarios, for example, MSDP peer creation, restart, or failback, you can shorten the TCP reconnection interval to accelerate convergence of the MSDP peer relationship.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the TCP reconnection interval of an MSDP peer.

ip msdp timer *interval*

The default TCP reconnection interval is **30** seconds.

1.5.7 Enabling MD5 Authentication on TCP Connections Between MSDP Peers

1. Overview

MD5 authentication is enabled on TCP connections between MSDP peers to prevent invalid TCP connections and improve MSDP security. To authenticate the ID of an MSDP peer, you can enable MD5 authentication on the TCP connection established with this MSDP peer.

2. Restrictions and Guidelines

- The MSDP peers must have the consistent configuration, and the ciphers must be the same; otherwise, TCP connections fail.
- If the encryption level is set to 7, the cipher text length must be an even number equal to or greater than 4; otherwise, the configuration fails.
- If the configuration or cipher changes, the local device does not stop the current session. Instead, it attempts to use a new cipher to retain the current session until timeout.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable MD5 authentication on TCP connections between MSDP peers.

ip msdp password peer *ipv4-peer-address* [*encryption-type*] *password-string*

The MD5 authentication function is disabled by default.

1.5.8 Configuring the Number of MSDP Peers Supported on a Device

1. Overview

You can configure the number of MSDP peers supported on a device. If the default number (64) cannot meet requirements, the number of the MSDP peers can be increased.

2. Restrictions and Guidelines

When the number of MSDP peers on the device exceeds the configured number, a notification is displayed to indicate configuration failure. In this case, you need to delete some peers to make the configuration take effect.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the number of MSDP peers supported on a device.

ip msdp peer-limit *peer-limit*

The maximum number of MSDP peers supported on a device is **64** by default.

1.6 Restricting SA Messages

1.6.1 Overview

MSDP peers share multicast source information by exchanging SA messages. Based on the actual network conditions, multicast packets encapsulated in SA messages can be defined, and SA requests and SA messages can be filtered.

1.6.2 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the TTL Value of Multicast Packets in SA Messages
- Enabling the Function of Filtering Source Information Released Locally
- Enabling the Function of Filtering Received SA Requests
- Enabling the Function of Filtering Received SA Messages
- Enabling the Function of Filtering Sent SA Messages
- Configuring SA Cache Capacity

1.6.3 Prerequisites

MSDP peer relationship is established between devices.

1.6.4 Configuring the TTL Value of Multicast Packets in SA Messages

1. Overview

If the interval of a multicast source for sending multicast data exceeds the timeout of an (S, G) entry, remote users cannot receive the multicast data sent by the multicast source. After the function of encapsulating multicast packets in SA messages is enabled on the source RP, the source RP encapsulates multicast packets in SA messages and sends them to the remote RPs. Upon receiving the messages, the remote RPs decapsulate the messages and transmit the packets in the local domain.

By configuring the time-to-live (TTL) value of multicast packets encapsulated in SA messages, you can control the sending of the multicast packets encapsulated in the SA messages.

- A multicast packet can be sent to MSDP peers only when the TTL value in the IP header of the multicast packet is equal to or greater than the preset TTL value.
- If the TTL value in the IP header of the multicast packet is smaller than the preset TTL value, the multicast packet is removed from the SA message and discarded before the SA message is sent to the MSDP peer.

Therefore, this function affects the sending of multicast packets in SA messages, and does not affect the sending of (S, G) information in the SA messages.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the TTL value of multicast packets in SA messages.

ip msdp ttl-threshold *ipv4-peer-address ttl-value*

The TTL value of the multicast packets in SA messages is not defined by default.

1.6.5 Enabling the Function of Filtering Source Information Released Locally

1. Overview

After source information registered on the local RP is filtered on an MSDP device, only allowed (S, G) information of the local or other domains can be released on the MSDP device.

2. Restrictions and Guidelines

- If the **list** keyword parameter is specified, only the (S, G) information matching this ACL is released.
- If the **route-map** keyword parameter is specified, only the (S, G) information matching this route map is released.
- If these two parameters are specified, only the (S, G) information matching the ACL and route map is released.
- If no parameter is specified, no (S, G) information is released.

3. Prerequisites

Before an IP multicast border is configured, ensure that the corresponding ACL or route map is created and an (S, G) range is specified.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Filter the source information released locally.

ip msdp redistribute [{ **list** *acl-name* | **list** *acl-number* } | **route-map** *route-map-name*] *

All (S, G) information registered on the local RP is released on the MSDP device by default.

1.6.6 Enabling the Function of Filtering Received SA Requests

1. Overview

An MSDP device gives a reply by default when the device receives an SA request. If you want to control the SA request and reply range, you can enable the SA request filtering function on the MSDP device to filter received SA requests.

2. Restrictions and Guidelines

- If the **list** keyword parameter is not specified, all the SA request messages are ignored.
- If the **list** keyword parameter is specified but this ACL is not configured, all SA request messages are ignored.
- If the **list** keyword parameter is specified and this ACL is configured, only the SA requests allowed by the ACL are accepted, and other SA requests are ignored.

3. Prerequisites

Before a received SA request is filtered, ensure that the corresponding ACL is created and a multicast group range is specified.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Filter received SA requests.

ip msdp filter-sa-request *ipv4-peer-address* [{ **list** *acl-name* | **list** *acl-number* }]

All SA request messages from MSDP peers are received and replied by default.

1.6.7 Enabling the Function of Filtering Received SA Messages

1. Overview

By default, SA messages are received and forwarded to other MSDP peers after they pass RPF check. You can configure filtering rules for incoming SA message on the MSDP device to filter received SA messages.

2. Restrictions and Guidelines

- If the function of filtering SA messages is enabled but no ACL or route map is configured, all incoming SA messages are filtered.
- If only one keyword (**list** or **route-map**) is specified and the multicast source (S, G) information in an SA message meets the rule specified by this keyword, this SA message is received.
- If only one keyword (**rp-list** or **rp-route-map**) is specified and the RP address contained in an SA message meets the rule specified by this keyword, this SA message is received.
- If two or more of the keywords (including **list**, **route-map, rp-list** and **rp-route-map**) are specified and the multicast source (S, G) information contained in an SA message meets the rules specified by these keywords, this SA message is received.

3. Prerequisites

Before an IP multicast border is configured, ensure that the corresponding ACL or route map is created and an (S, G) range is specified.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Filter received SA messages.

ip msdp sa-filter in *ipv4-peer-address* [{ **list** *acl-name* | **list** *acl-number* } | **route–map** *route-map-name* | { **rp-list** *acl-name* | **rp-list** *acl-number* } | **rp-route-map** *rp-route-map-name*] *

All SA messages from MSDP peers are received by default.

1.6.8 Enabling the Function of Filtering Sent SA Messages

1. Overview

By default, SA messages are received and forwarded to other MSDP peers after they pass RPF check. You can configure outgoing SA message filtering rules on the MSDP device to filter SA messages to be forwarded.

2. Restrictions and Guidelines

- If the function of filtering sent SA messages is enabled but no ACL or route map is specified, no SA message is sent to other MSDP peers.
- If only one of the keywords (including **list**, **route-map**, **rp-list**, and **rp-route-map**) is specified and the multicast source (S, G) information in an SA message meets the rule specified by this keyword, this SA message is forwarded to other MSDP peers.
- If two or more of the keywords (including **list**, **route-map**, **rp-list**, and **rp-route-map**) are specified and the multicast source (S, G) information in an SA message meets the rules specified by these keywords, this SA message is forwarded to other MSDP peers.

3. Prerequisites

Before an IP multicast border is configured, ensure that the corresponding ACL or route map is created and an (S, G) range is specified.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Filter sent SA messages.

ip msdp sa-filter out *ipv4-peer-address* [{ **list** *acl-name* | **list** *acl-number* } | **route–map** *route-map-name* | { **rp-list** *acl-name* | **rp-list** *acl-number* } | **rp-route-map** *rp-route-map*] *

By default, all SA messages are forwarded to MSDP peers.

1.6.9 Configuring SA Cache Capacity

1. Overview

If an SA cache is used to cache SA messages, the (S, G) entries contained in the SA messages are cached in the SA cache. When a device receives a new join message, the device searches for the SA cache to reduce the

delay time of obtaining the multicast information. The more (S, G) entries cached, the greater the used memory space. To suppress SA message flooding, you can limit the number of SA cache entries from a specified MSDP peer or a device.

2. Restrictions and Guidelines

- You are advised to configure the SA cache capacity when you start a device.
- During MSDP running,
  - if the capacity is increased, the adjustment does not affect the SA cache entries that are originally learned.
  - If the capacity is decreased, all SA cache entries learned and initiated must be deleted and re-learned.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Limit the number of SA cache entries from a specified MSDP peer.

ip msdp sa-limit *ipv4-peer-address sa-limit*

The number of SA cache entries from a specified MSDP peer is not limited by default.

(4) (Optional) Configure the SA cache capacity supported on a device.

ip msdp global-sa-limit *sa-limit*

The default SA cache capacity supported on a device is **1024**.

1.7 Configuring an Anycast RP

1.7.1 Overview

RPs in a PIM-SM domain use the same RP address to serve the same group. MSDP peer relationship is established between RPs so that multicast sources and receivers can register with and join the nearest RP. The RPs implement redundancy and load sharing and help accelerate convergence of multicast routes.

1.7.2 Prerequisites

Basic multicast functions are enabled in the PIM-SM domain and multiple RPs are configured for the domain.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Establish an MSDP peer relationship.

ip msdp peer *ipv4-peer-address* **connect-source** *interface-type interface-number*

No MSDP peer is added by default.

(4) Modify the RP address in SA messages.

ip msdp originator-id *interface-type interface-number*

By default, no primary address of an interface is specified as the initiator address in SA messages.

1.8 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

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

Table 1-2 Monitoring

Command	Purpose
clear ip msdp peer *ipv4-peer-address*	Resets the TCP connection with a specified MSDP peer.
clear ip msdp sa-cache [*ipv4-group-address*]	Clears the SA cache.
clear ip msdp statistics [*ipv4-peer-address*]	Clears the statistics of MSDP peers.
show ip msdp count [*as-number*]	Displays the number of sources and the number of groups generated by SA messages.
show ip msdp mesh-group	Displays information of a mesh group.
show ip msdp peer [*ipv4-peer-address*]	Displays detailed information about MSDP peers.
show ip msdp rpf-peer *ipv4-address*	Displays information about the MSDP RPF peer corresponding to the address of a specified initiator.
show ip msdp sa-cache [*ipv4-group-address* **|** *ipv4-source-address*] [*ipv4-group-address* **|** *ipv4-source-address*] [*as-number*]	Displays learned (S, G) information.
show ip msdp sa-originated	Displays (S, G) information initiated by the local device.
show ip msdp summary	Displays summary information of all MSDP peers.
debug ip msdp peer	Debugs MSDP peers.

1.9 Configuration Examples

1.9.1 Enabling Basic Functions of MSDP

1. Requirements

MSDP peers are configured in different domains to connect the RPs. Multicast source information can be shared to other RPs.

2. Topology

Figure 1-7 Topology for Basic Functions of MSDP

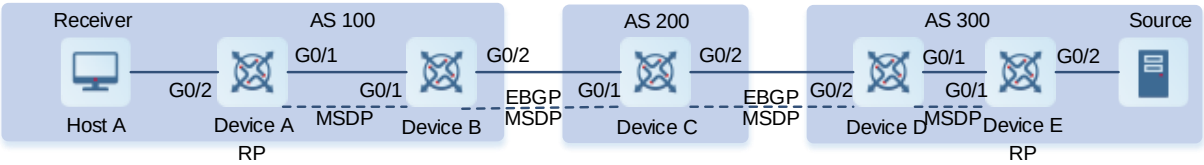


Table 1-3 Description of the Topology

Device	Interface	IP Address	Remarks
Device A	G0/1	10.110.1.1/24	-
	Loopback0	10.10.10.10/32	RP address, which is used to establish an MSDP connection.
Device B	G0/1	10.110.1.2/24	-
	G0/2	10.110.2.1/24	BSR border
	Loopback0	20.20.20.20/32	Used to establish the EBGP and MSDP connections.
Device C	G0/1	10.110.2.2/24	BSR border
	G0/2	10.110.3.1/24	BSR border
	Loopback0	30.30.30.30/32	Used to establish the EBGP and MSDP connections.
Device D	G0/2	10.110.3.2/24	BSR border
	G0/1	10.110.4.1/24	-
	Loopback0	40.40.40.40/32	Used to establish the EBGP and MSDP connections.
Device E	G0/1	10.110.4.2/24	-
	Loopback0	50.50.50.50/32	RP address, which is used to establish an MSDP connection.

3. Notes

- Configure an IP address for an interface.
- Enable OSPF in each AS. Establish EBGP peer relationship between AS 200 and AS 100 and between AS

200 and AS 300, and introduce learned BGP and OSPF routes.

- Enable PIM-SM in each AS, configure C-BSRs and C-RPs, and configure the BSR border.
- Establish the MSDP peer relationship between EBGP peers and between the RP and EBGP peers.

Caution

The IP address and local interface of the MSDP peer must be the same as those of the EBGP peer.

4. Procedure

(1) Configure an IP address for each interface (omitted).

(2) Enable OSPF in each AS. Establish EBGP peer relationship between AS 200 and AS 100 and between AS 200 and AS 300, and introduce BGP and OSPF (omitted). For the omitted information, see *Configuring OSPFv2* and *Configuring BGP*

(3) Enable PIM-SM in each AS, configure C-BSRs and C-RPs, and configure the BSR border.

Configure device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# ip multicast-routing
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface loopback 0
Device A(config-if-Loopback 0)# ip pim sparse-mode
Device A(config-if-Loopback 0)# exit
Device A(config)# ip pim rp-candidate loopback 0
Device A(config)# ip pim bsr-candidate loopback 0
```

Configure device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# ip multicast-routing
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device B(config-if-GigabitEthernet 0/2)# ip pim bsr-border
Device B(config-if-GigabitEthernet 0/2)# exit
Device B(config)# interface loopback 0
Device B(config-if-Loopback 0)# ip pim sparse-mode
Device B(config-if-Loopback 0)# exit
```

Configure device C.

```
Device C>enable
Device C# configure terminal
```

```
Device C(config)# ip multicast-routing
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device C(config-if-GigabitEthernet 0/1)# ip pim bsr-border
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface GigabitEthernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device C(config-if-GigabitEthernet 0/2)# ip pim bsr-border
Device C(config-if-GigabitEthernet 0/2)# exit
Device C(config)# interface loopback 0
Device C(config-if-loopback 0)# ip pim sparse-mode
Device C(config-if-loopback 0)# exit
```

Configure device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# ip multicast-routing
Device D(config)# ip pim ssm default
Device D(config)# interface GigabitEthernet 0/1
Device D(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device D(config-if-GigabitEthernet 0/1)# exit
Device D(config)# interface GigabitEthernet 0/2
Device D(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device D(config-if-GigabitEthernet 0/2)# ip pim bsr-border
Device D(config-if-GigabitEthernet 0/2)# exit
Device D(config)# interface loopback 0
Device D(config-if-Loopback 0)# ip pim sparse-mode
Device D(config-if-Loopback 0)# exit
```

Configure device E.

```
Device E> enable
Device E# configure terminal
Device E(config)# ip multicast-routing
Device E(config)# interface GigabitEthernet 0/1
Device E(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device E(config-if-GigabitEthernet 0/1)# exit
Device E(config)# interface loopback 0
Device E(config-if-Loopback 0)# ip pim sparse-mode
Device E(config-if-Loopback 0)# exit
Device E(config)# ip pim rp-candidate loopback 0
Device E(config)# ip pim bsr-candidate loopback 0
```

(4) Establish the MSDP peer relationship between EBGP peers and between the RP and EBGP peers.

Configure device A.

```
Device A(config)# ip msdp peer 10.10.10.10 connect-source loopback 0
```

Configure device B.

```
Device B(config)# ip msdp peer 10.10.10.10 connect-source loopback 0
```

```
Device B(config)# ip msdp peer 30.30.30.30 connect-source loopback 0
```

Configure device C.

```
Device C(config)# ip msdp peer 20.20.20.20 connect-source loopback 0
Device C(config)# ip msdp peer 40.40.40.40 connect-source loopback 0
```

Configure device D.

```
Device D(config)# ip msdp peer 30.30.30.30 connect-source loopback 0
Device D(config)# ip msdp peer 50.50.50.50 connect-source loopback 0
```

Configure device E.

```
Device E(config)# ip msdp peer 50.50.50.50 connect-source loopback 0
```

5. Verification

(1) Use the multicast source to send a packet (200.200.200.200, 225.1.1.1). After a host joins the group 225.1.1.1, this host can receive this packet.

(2) Display the status and SA message of the MSDP peer on device D.

```
Device D# show ip msdp summary
Msdp Peer Status Summary
Peer Address   As   State   Uptime/Downtime   Reset-Count   SA-Count
Peer-Description
30.30.30.30    200  Up     00:01:420                   1         No description

Device D# show ip msdp sa-cache
MSDP Source-Active Cache: 1 entries
  (200.200.200.200,225.1.1.1),RP:10.10.10.10,(M)BGP/AS 100, 00:00:18/00:01:57,
Peer 30.30.30.30
Learned from peer 30.30.30.30, RPF peer 30.30.30.30,
SAs received: 1, Encapsulated data received: 1
```

6. Configuration Files

- Device A configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface Loopback 0
 ip pim sparse-mode
!
ip msdp peer 10.10.10.10 connect-source Loopback 0
!
ip pim bsr-candidate Loopback 0
ip pim rp-candidate Loopback 0
!
```

- Device B configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
 ip pim bsr-border
!
interface Loopback 0
 ip pim sparse-mode
!
ip msdp peer 10.10.10.10 connect-source Loopback 0
ip msdp peer 30.30.30.30 connect-source Loopback 0
!
```

- Device C configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
 ip pim bsr-border
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
 ip pim bsr-border
!
interface Loopback 0
 ip pim sparse-mode
!
ip msdp peer 20.20.20.20 connect-source Loopback 0
ip msdp peer 40.40.40.40 connect-source Loopback 0
!
```

- Device D configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
```

```
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
 ip pim bsr-border
!
interface Loopback 0
 ip pim sparse-mode
!
ip pim ssm default
!
ip msdp peer 30.30.30.30 connect-source Loopback 0
ip msdp peer 50.50.50.50 connect-source Loopback 0
!
```

- Device E configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface Loopback 0
 ip pim sparse-mode
!
ip msdp peer 50.50.50.50 connect-source Loopback 0
!
ip pim bsr-candidate Loopback 0
ip pim rp-candidate Loopback 0
!
```

7. Common Errors

- The BSR border is not configured, or is not configured on a correct interface.
- PIM-SM is not enabled on the local interface and the peer interface on which MSDP peer connection is established.
- SA messages fail the peer RPF check.

1.9.2 Configuring an Anycast RP

1. Requirements

There are multiple RPs in a PIM domain. After an anycast RP based on MSDP peers is configured, receivers can join the nearest RP, and the multicast source can register with the nearest RP to implement load sharing between the RPs.

2. Topology

Figure 1-8 Anycast RP Topology

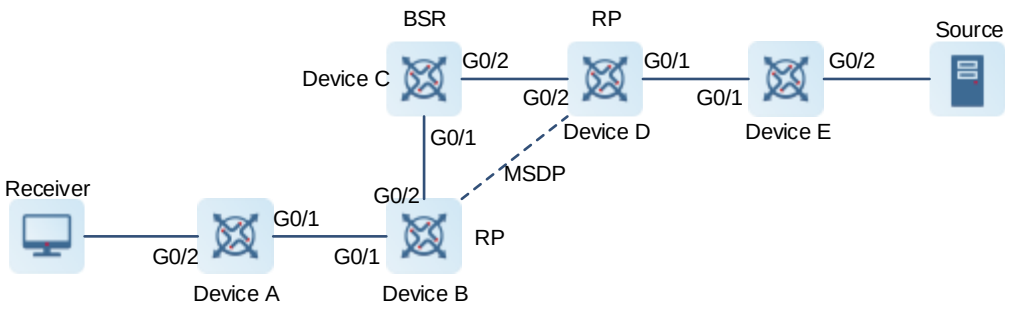


Table 1-4 Description of the Topology

Device	Interface	IP Address	Remarks
Device A	G0/1	10.110.1.1/24	
	G0/2	10.110.2.1/24	
Device B	G0/1	10.110.1.2/24	
	G0/2	10.110.3.1/24	
	Loopback0	10.10.10.10/32	A C-RP is configured.
	Loopback1	30.30.30.30/32	Used to establish an MSDP connection and modify the RP address in the SA message.
Device C	G0/1	10.110.3.2/24	
	G0/2	10.110.4.1/24	
	Loopback0	100.100.100.100/32	A C-BSR is configured.
Device D	G0/1	10.110.5.1/24	
	G0/2	10.110.4.2/24	
	Loopback0	10.10.10.10/32	A C-RP is configured.
	Loopback1	20.20.20.20/32	Used to establish an MSDP connection and modify the RP address in the SA message.
Device E	G0/1	10.110.5.2/24	
	G0/2	10.110.6.1/24	

3. Notes

- Configure an IP address for each interface.

- Enable OSPF in each AS.
- Enable PIM-SM in each AS, and configure C-BSRs and C-RPs.
- Establish the MSDP peer relationship between RPs, and modify the RP address in the SA message.
- Configure a mesh group.

4. Procedure

(1) Configure an IP address for each interface (omitted).

(2) Enable OSPF in each AS (omitted). For the omitted information, see *Configuring OSPFv2*.

(3) Enable PIM-SM in each AS, and configure C-BSRs and C-RPs.

Configure device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# ip multicast-routing
Device A(config)# interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface GigabitEthernet 0/2
Device A(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device A(config-if-GigabitEthernet 0/2)# exit
```

Configure device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# ip multicast-routing
Device B(config)# interface GigabitEthernet 0/1
Device B(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device B(config-if-GigabitEthernet 0/1)# exit
Device B(config)# interface GigabitEthernet 0/2
Device B(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device B(config-if-GigabitEthernet 0/2)# exit
Device B(config)# interface loopback 0
Device B(config-if-Loopback 0)# ip pim sparse-mode
Device B(config-if-Loopback 0)# exit
Device B(config)# interface loopback 1
Device B(config-if-Loopback 1)# ip pim sparse-mode
Device B(config-if-Loopback 1)# exit
Device B(config)# ip pim rp-candidate loopback 0
```

Configure device C.

```
Device C> enable
Device C# configure terminal
Device C(config)# ip multicast-routing
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device C(config-if-GigabitEthernet 0/1)# exit
```

```
Device C(config)# interface GigabitEthernet 0/2
Device C(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device C(config-if-GigabitEthernet 0/2)# exit
Device C(config)# interface loopback 0
Device C(config-if-Loopback 0)# ip pim sparse-mode
Device C(config-if-Loopback 0)# exit
Device C(config)# ip pim bsr-candidate loopback0
```

Configure device D.

```
Device D> enable
Device D# configure terminal
Device D(config)# ip multicast-routing
Device D(config)# interface GigabitEthernet 0/1
Device D(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
Device D(config-if-GigabitEthernet 0/1)# exit
Device D(config)# interface GigabitEthernet 0/2
Device D(config-if-GigabitEthernet 0/2)# ip pim sparse-mode
Device D(config-if-GigabitEthernet 0/2)# exit
Device D(config)# interface loopback 0
Device D(config-if-Loopback 0)# ip pim sparse-mode
Device D(config-if-Loopback 0)# exit
Device D(config)# interface loopback 1
Device D(config-if-Loopback 1)# ip pim sparse-mode
Device D(config-if-Loopback 1)# exit
Device D(config)# ip pim rp-candidate loopback 0
```

Configure device E.

```
Device E>enable
Device E#configure terminal
Device E(config)#ip multicast-routing
Device E(config)#interface GigabitEthernet 0/1
Device E(config-if-GigabitEthernet 0/1)#ip pim sparse-mode
Device E(config-if-GigabitEthernet 0/1)# exit
Device E(config)#interface GigabitEthernet 0/2
Device E(config-if-GigabitEthernet 0/2)#ip pim sparse-mode
Device E(config-if-GigabitEthernet 0/2)# exit
```

(4) Establish the MSDP peer relationship between RPs, and modify the RP address in the SA message.

Configure device D.

```
Device D(config)# ip msdp peer 30.30.30.30 connect-source loopback 1
Device D(config)# ip msdp originator-id loopback 1
```

Configure device B.

```
Device B(config)# ip msdp peer 20.20.20.20 connect-source loopback 1
Device B(config)# ip msdp originator-id loopback 1
```

(5) Configure a mesh group.

Configure device D.

```
Device D(config)# ip msdp mesh-group mesh-name 30.30.30.30
```

Configure device B.

```
Device B(config)# ip msdp mesh-group mesh-name 20.20.20.20
```

5. Verification

(1) Use the multicast source to send a packet (6.6.6.6, 225.1.1.1). After a host joins the group 225.1.1.1, this host can receive this packet.

(2) Display the status and SA message of the MSDP peer on device B.

Run the **show ip msdp summary** command to display status of the peers.

```
Device B# show ip msdp summary
Msdp Peer Status Summary
Peer Address   As       State   Uptime/Downtime   Reset-Count   SA-Count
Peer-Description
20.20.20.20    Unknown   Up      00:01:420                   1         No
description
```

Run the **show ip msdp sa-cache** command to display SA messages of the peers.

```
Device B# show ip msdp sa-cache
MSDP Source-Active Cache: 1 entries
  (6.6.6.6,225.1.1.1),RP:10.10.10.10,(M)BGP/AS unknown, 00:00:18/00:01:57, Peer
20.20.20.20
```

6. Configuration Files

- Device A configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
!
```

- Device B configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
```

```
 ip pim sparse-mode
!
interface Loopback 0
 ip pim sparse-mode
!
interface Loopback 1
 ip pim sparse-mode
!
ip msdp originator-id Loopback 1
ip msdp peer 20.20.20.20 connect-source Loopback 1
ip msdp mesh-group mesh-name 20.20.20.20
!
ip pim rp-candidate Loopback 0
!
```

- Device C configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
!
interface Loopback 0
 ip pim sparse-mode
!
ip pim bsr-candidate Loopback 0
!
```

- Device D configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
!
interface Loopback 0
 ip pim sparse-mode
```

```
!
interface Loopback 1
 ip pim sparse-mode
!
ip msdp originator-id Loopback 1
ip msdp peer 30.30.30.30 connect-source Loopback 1
ip msdp mesh-group mesh-name 30.30.30.30
!
ip pim rp-candidate Loopback 0
!
```

- Device E configuration file

```
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ip pim sparse-mode
!
```

7. Common Errors

- The C-BSRs and C-RPs are configured on the same interface.
- The RP address in the SA message is not modified.
- SA messages cannot pass the peer RPF check.

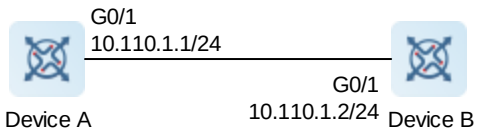
1.9.3 Enabling MD5 Authentication

1. Requirements

MD5 authentication is enabled on TCP connections between MSDP peers, and the number of SA cache entries from a specified MSDP peer is limited to prevent invalid TCP connections and improve MSDP security.

2. Topology

Figure 1-9 Topology of MD5 Authentication



3. Notes

- Establish the MSDP peer relationship between device A and device B.
- Enable MD5 authentication for the peer on device A.

- After MSDP timeout, configure the MD5 cipher of the peer on device B, which is the same as the cipher on device A. Then, the session is reconnected.
- Set the number of SA cache entries from the peer 10.110.1.2 to 10.

4. Procedure

(1) Configure IP addresses on interfaces of device A and device B, and enable basic functions of PIM-SM on the devices (omitted).

(2) Establish the MSDP peer relationship between device A and device B.

Add device B as an MSDP peer on device A.

```
Device A> enable
Device A# configure
Device A(config)# ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
```

Add device A as an MSDP peer on device B.

```
Device B> enable
Device B# configure
Device B(config)# ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
```

(3) Enable MD5 authentication for the peer on device A, and set the encryption level to 0 and the cypher to password123.

```
Device A(config)# ip msdp password peer 10.110.1.2 0 password123
```

(4) After MSDP timeout, enable MD5 authentication for the peer on device B, and set the encryption level and cypher to be consistent with those on device A.

```
Device B(config)# ip msdp password peer 10.110.1.1 0 password123
```

(5) Set the number of SA cache entries from the peer 10.110.1.2 to 10.

```
Device A(config)# ip msdp sa-limit 10.110.1.2 10
```

5. Verification

(1) After the MSDP peer relationship is established between device A and device B, the peer status is up.

Check whether the status of the peer 10.110.1.2 is up on device A.

```
Device A# show ip msdp peer
MSDP PEER 10.110.1.2 (No description), AS unknown
  Connection status:
    State: Up, Resets: 0, Connection source: GigabitEthernet 0/7 (10.110.1.1)
    Uptime(Downtime): 00:01:14, Message sent/received: 2/2
    Input messages discarded: 0
    Connection and counters cleared 00:01:44 ago
    Local Address of connection: 10.110.1.1
  SA Filtering:
    Input (S,G) Access-list filter: None
    Input (S,G) route-map filter: None
    Input RP Access-list filter: None
    Input RP Route-map filter: None
    Output (S,G) Access-list filter: None
```

```
    Output (S,G) Route-map filter: None
    Output RP Access-list filter: None
    Output RP Route-map filter: None
  SA-Requests:
    Input filter: None
  Peer ttl threshold: 0
  SAs learned from this peer: 0, SAs limit: No-limit
  Message counters:
    SA messages discarded: 0
    SA messages in/out: 0/0
    SA Requests discarded/in: 0/0
    SA Responses out: 0
    Data Packets in/out: 0/0
```

Check whether the status of the peer 10.110.1.1 is up on device B.

```
Device B# show ip msdp peer
MSDP PEER 10.110.1.1 (No description), AS unknown
  Connection status:
    State: Up, Resets: 0, Connection source: GigabitEthernet 0/1 (10.110.1.2)
    Uptime(Downtime): 00:00:05, Message sent/received: 1/1
    Input messages discarded: 0
    Connection and counters cleared 00:00:14 ago
    Local Address of connection: 10.110.1.2
  SA Filtering:
    Input (S,G) Access-list filter: None
    Input (S,G) route-map filter: None
    Input RP Access-list filter: None
    Input RP Route-map filter: None
    Output (S,G) Access-list filter: None
    Output (S,G) Route-map filter: None
    Output RP Access-list filter: None
    Output RP Route-map filter: None
  SA-Requests:
    Input filter: None
  Peer ttl threshold: 0
  SAs learned from this peer: 0, SAs limit: No-limit
  Message counters:
    SA messages discarded: 0
    SA messages in/out: 0/0
    SA Requests discarded/in: 0/0
```

(2) After MD5 authentication is enabled for the peer on device A, run the **show ip msdp peer** command to check whether the peer relationship between device A and device B is disconnected and the peer is down.

(3) After MD5 authentication is enabled for the peer on device B, run the **show ip msdp peer** command to check whether the peer relationship between device A and device B is established and the peer is up again.

(4) Set the number of SA cache entries from the peer 10.110.1.2 to 10 on device A, and send 20 (S, G) entries to device B. A message is displayed on device A, indicating that the number of entries exceeds the limit.

6. Configuration Files

- Device A configuration file

```
!
ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
ip msdp password peer 10.110.1.2 0 password123
ip msdp sa-limit 10.110.1.2 10
!
```

- Device B configuration file

```
!
ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
ip msdp password peer 10.110.1.1 0 password123
!
```

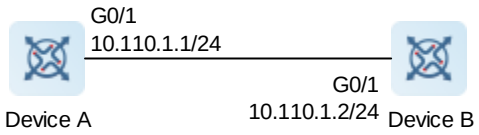
1.9.4 Managing MSDP Peers

1. Requirements

MSDP peer information is managed and configured, including configuring peer description information and disabling peer connections.

2. Topology

Figure 1-10 Topology of MSDP Peer Management



3. Notes

- Establish MSDP peer relationship between device A and device B.
- On device A, configure the peer description of device B as "peer-router-B".
- After 60 seconds, on device A, disable the peer device B.

4. Procedure

(1) Configure IP addresses on interfaces of device A and device B, and enable basic functions of PIM-SM on the devices (omitted).

(2) Establish the MSDP peer relationship between device A and device B.

Add device B as an MSDP peer on device A.

```
Device A> enable
Device A# configure
Device A(config)# ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
```

Add device A as an MSDP peer on device B.

```
Device B> enable
```

```
Device B# configure
Device B(config)# ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
```

(3) On device A, configure the peer description of device B as "peer-router-B".

```
Device A(config)# ip msdp description 10.110.1.2 peer-router-B
```

(4) After 60 seconds, on device A, disable the peer device B.

```
Device A(config)# ip msdp shutdown 10.110.1.2
```

5. Verification

Run the **show ip msdp peer** command to display the summary information of a specified peer, including the description and connection status of this MSDP peer.

```
Device A# show ip msdp peer 10.110.1.2
MSDP PEER 10.110.1.2 (peer-router-B), AS unknown
  Connection status:
    State: Up, Resets: 3, Connection source: GigabitEthernet 0/1 (10.110.1.1)
    Uptime(Downtime): 00:30:39, Message sent/received: 50/50
    Input messages discarded: 0
    Connection and counters cleared 00:51:06 ago
    Local Address of connection: 10.110.1.1
  SA Filtering:
    Input (S,G) Access-list filter: None
    Input (S,G) route-map filter: None
    Input RP Access-list filter: None
    Input RP Route-map filter: None
    Output (S,G) Access-list filter: None
    Output (S,G) Route-map filter: None
    Output RP Access-list filter: None
    Output RP Route-map filter: None
  SA-Requests:
    Input filter: None
  Peer ttl threshold: 0
  SAs learned from this peer: 0, SAs limit: No-limit
  Message counters:
    SA messages discarded: 0
    SA messages in/out: 0/0
    SA Requests discarded/in: 0/0
    SA Responses out: 0
    Data Packets in/out: 0/0
```

6. Configuration Files

- Device A configuration file

```
!
ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
ip msdp shutdown 10.110.1.2
ip msdp description 10.110.1.2 peer-router-B
!
```

- Device B configuration file

```
!
ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
!
```

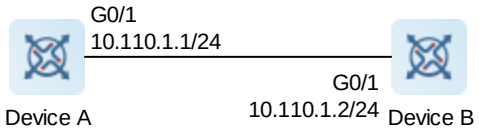
1.9.5 Modifying Protocol Parameters

1. Requirements

In some application scenarios, for example, MSDP peer creation, restart, or failback, you can shorten the TCP reconnection interval to accelerate convergence of the MSDP peer relationship.

2. Topology

Figure 1-11 Topology for Protocol Parameter Modification



3. Notes

- Establish the MSDP peer relationship between device A and device B.
- Set the MSDP peer reconnection interval to 20 seconds on device A.

4. Procedure

(1) Configure IP addresses on interfaces of device A and device B, and enable basic functions of PIM-SM on the devices (omitted).

(2) Establish the MSDP peer relationship between device A and device B.

Add device B as an MSDP peer on device A.

```
Device A> enable
Device A# configure
Device A(config)# ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
```

Add device A as an MSDP peer on device B.

```
Device B> enable
Device B# configure
Device B(config)# ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
```

(3) Set the MSDP peer reconnection interval to 20 seconds on device A.

```
Device(config)# ip msdp timer 20
```

5. Verification

(1) Disable the MSDP peer on device B, and enable the MSDP peer again immediately.

```
Device B(config)# ip msdp shutdown 10.110.1.1
Device B(config)# no ip msdp shutdown 10.110.1.1
```

(2) Check whether the peer on device B can be reconnected in 20 seconds.

```
Device B# show ip msdp peer 10.110.1.1
MSDP PEER 10.110.1.1 (peer-a), AS unknown
  Connection status:
    State: Up, Resets: 3, Connection source: GigabitEthernet 0/1 (10.110.1.2)
    Uptime(Downtime): 00:00:41, Message sent/received: 20/20
    Input messages discarded: 0
    Connection and counters cleared 01:37:02 ago
    Local Address of connection: 10.110.1.2
  SA Filtering:
    Input (S,G) Access-list filter: None
    Input (S,G) route-map filter: None
    Input RP Access-list filter: None
    Input RP Route-map filter: None
    Output (S,G) Access-list filter: None
    Output (S,G) Route-map filter: None
    Output RP Access-list filter: None
    Output RP Route-map filter: None
  SA-Requests:
    Input filter: None
  Peer ttl threshold: 0
  SAs learned from this peer: 0, SAs limit: No-limit
  Message counters:
    SA messages discarded: 0
    SA messages in/out: 0/0
    SA Requests discarded/in: 0/0
    SA Responses out: 0
    Data Packets in/out: 0/0
```

6. Configuration Files

- Device A configuration file

```
!
ip msdp timer 20
ip msdp peer 10.110.1.2 connect-source gigabitEthernet 0/1
!
```

- Device B configuration file

```
!
ip msdp peer 10.110.1.1 connect-source gigabitEthernet 0/1
!
```

Contents

1 Configuring IPv6 Multicast Route Management 3
1.1 Introduction 3
1.1.1 IPv6 Multicast Routing and Forwarding 3
1.1.2 RPF Check 3
1.1.3 Protocols and Standards 6
1.2 Configuration Task Summary 6
1.3 Prerequisites 6
1.4 Configuring Basic Functions of IPv6 Multicast 6
1.4.1 Overview 6
1.4.2 Restrictions and Guidelines 6
1.4.3 Prerequisites 7
1.4.4 Procedure 7
1.5 Configuring the Maximum Number of Entries in an IPv6 Multicast Routing Table 7
1.5.1 Overview 7
1.5.2 Restrictions and Guidelines 7
1.5.3 Prerequisites 7
1.5.4 Procedure 7
1.6 Configuring an IPv6 Multicast Border 8
1.6.1 Overview 8
1.6.2 Restrictions and Guidelines 8
1.6.3 Prerequisites 8
1.6.4 Procedure 8

1.7 Configuring an IPv6 Static Multicast Route 9
1.7.1 Overview 9
1.7.2 Restrictions and Guidelines 9
1.7.3 Prerequisites 9
1.7.4 Procedure 9
1.8 Enabling Forced Forwarding of Multicast Packets by Software 9
1.8.1 Overview 9
1.8.2 Restrictions and Guidelines 9
1.8.3 Prerequisites 10
1.8.4 Procedure 10
1.9 Enabling L2 Direction Control for Multicast Streams 10
1.9.1 Overview 10
1.9.2 Restrictions and Guidelines 10
1.9.3 Prerequisites 10
1.9.4 Procedure 10
1.10 Configuring RPF Route Selection Based on the Longest Match Rule 11
1.10.1 Overview 11
1.10.2 Restrictions and Guidelines 11
1.10.3 Prerequisites 11
1.10.4 Procedure 11
1.11 Monitoring 11
1.12 Configuration Examples 13
1.12.1 Configuring an IPv6 Static Multicast Route to Modify the RPF Route 13
1.12.2 Configuring a Static Multicast Route to Connect the RPF Route 19

1 Configuring IPv6 Multicast Route Management

1.1 Introduction

Multicast route management covers how to create and modify multicast routes to control multicast packet forwarding and how to detect and maintain correctness of multicast forwarding paths. Multicast route management mainly includes the static multicast routing and reverse path forwarding (RPF) check features. Static multicast routing is used to modify or connect RPF routes, and RPF check is used to ensure that multicast data is forwarded on correct paths.

1.1.1 IPv6 Multicast Routing and Forwarding

An IPv6 multicast routing table includes MLD group entries, multicast protocol routing entries, multicast routing entries, and multicast hardware forwarding entries. These entries are maintained by different multicast routing protocols in the multicast network. The optimal IPv6 multicast routes are delivered to the hardware forwarding table and used to guide IPv6 multicast data forwarding. The RPF mechanism ensures that multicast data is forwarded on correct paths.

- MLD group entries: They are created when a host sends MLD join packets and used to maintain group member information and ask the multicast routing protocol to create (S, G) or (*, G) entries.
- Multicast protocol routing entries: They function as basis of multicast routing and forwarding and are maintained by different multicast routing protocols (the most widely applied protocol is PIM).
- Multicast routing entries: They are generated by the multicast routing management module and delivered to a multicast forwarding table. Different multicast routing protocols can be summarized based on the multicast routing entries to select an optimal route.
- Hardware forwarding entries: They are generated based on routing tables and used to guide multicast data forwarding.

1.1.2 RPF Check

1. Basic Principles

In unicast routing and forwarding, a device gets to know the outbound interface of packets based on the destination address. In multicast routing and forwarding, the destination address in multicast packets is a multicast address, based on which, a receiver address cannot be determined. However, the source address in multicast packets is determined and based on this source address, multicast packets can be forwarded on correct paths.

When receiving a multicast packet, a multicast device queries the unicast route of the multicast source based on the source address in the multicast packet and checks whether the outbound interface of this unicast route is consistent with the inbound interface of the multicast packet. If yes, it is considered that this multicast packet is forwarded on a correct path. The inbound interface of the multicast packet is referred to as an RPF interface.

2. RPF Check Procedure

Unicast route, MBGP route, and static multicast route are the basis of RPF check. If these three types of routing entries exist on a multicast device, the multicast device performs the following checks in order after receiving a multicast packet:

(1) Select an optimal route from each of the three types of routing entries, respectively, based on the source address in the packet.

- The outbound interface of a unicast route is an RPF interface and the next hop is an RPF neighbor.
- The outbound interface of an MBGP route is an RPF interface and the next hop is an RPF neighbor.
- The static multicast route is manually configured and an RPF interface and neighbor are specified.

(2) Select one route out of the three optimal routes as the RPF route. The selection rule is as follows:

- If the longest match rule is not configured for selecting an RPF route, the one with the highest priority is selected as the RPF route. If the three routes have the same priority, the RPF route is selected in the order of static multicast route, MBGP route, and unicast route.
- If the longest match rule is configured for selecting an RPF route, the one with the longest match is selected as the RPF route. If the three routes have the same mask, the one with the highest priority is selected as the RPF route. If they have the same priority, the RPF route is selected in the order of static multicast route, MBGP route, and unicast route.

(3) Compare the RPF interface of the RPF route with the inbound interface of the multicast packet.

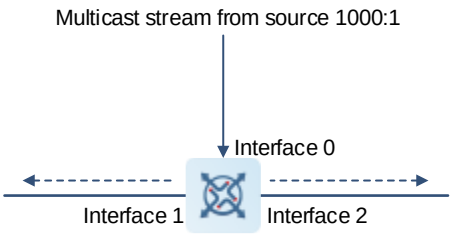
- If they are consistent, the route passes the RPF check and the multicast packet is forwarded to the downlink devices.
- If they are inconsistent, the route fails the RPF check and the received multicast packet is discarded.

Table 1-1 Routing Table on a Multicast Device

IP Routing Table	
Network	**Interface**
1000::/64	Interface 0
2000::/64	Interface 1
3000::/64	Interface 2

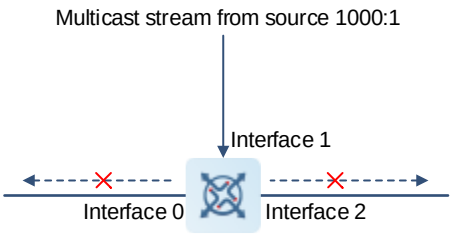
As shown in Figure 1-1, the multicast device receives a multicast packet from the source 1000::1 through interface 0 and as listed in Table 1-1, the outbound interface of the route to the source 1000::1 is also interface 0. The outbound interface of the route is consistent with the inbound interface of the multicast packet. The route passes the RPF check and the multicast packet is forwarded on the correct path.

Figure 1-1 Topology of RPF Check Success



As shown in Figure 1-2, the multicast device receives a multicast packet from the source 1000::1 through interface 1 and the outbound interface of the route to the source 1000::1 is Interface 0. The outbound interface of the route is inconsistent with the inbound interface of the multicast packet. The route fails the RPF check and the multicast packet is discarded.

Figure 1-2 Topology of RPF Check Failure



3. Application Scenarios of RPF Check in Multicast Forwarding

A multicast device ensures that multicast packets are forwarded on correct paths and avoids loops on the forwarding paths based on the RPF check mechanism. In actual applications, if the multicast device performs RPF check each time it receives a multicast packet, the multicast device is overloaded. Therefore, upon receiving a multicast packet, the multicast device checks for corresponding (S, G) hardware forwarding entry, rather than performs RPF check. The checking process is as follows:

- If no (S, G) hardware forwarding entry exists, the multicast device performs RPF check, uses the RPF interface as an inbound interface, creates a multicast routing entry, and delivers the entry to the multicast forwarding table.
  - If the route passes the RPF check, the inbound interface of the multicast packet is consistent with the RPF interface. The multicast packet is forwarded to all the outbound interfaces in the forwarding table.
  - If the route fails the RPF check, the inbound interface of the multicast packet is inconsistent with the RPF interface. The multicast packet is discarded.
- If (S, G) hardware forwarding entries exist, the multicast device checks whether the inbound interface in the forwarding entry is consistent with the inbound interface of the multicast packet.
  - If they are consistent, the multicast packet is forwarded to all the outbound interfaces.
  - If they are inconsistent, the multicast device performs RPF check. If the RPF interface is consistent with the inbound interface in the hardware forwarding entry, the source path of the packet is incorrect but the (S, G) entry is correct. The multicast packet is discarded. If the RPF interface is inconsistent with the inbound interface in the hardware forwarding entry, the (S, G) entry expired. The inbound interface in

the entry is updated as an RPF interface. Then, the multicast device checks whether the RPF interface is consistent with the inbound interface of the packet. If they are consistent, this multicast packet is forwarded to all outbound interfaces in the forwarding table. Otherwise, this multicast packet is discarded.

1.1.3 Protocols and Standards

- RFC2710: Multicast Listener Discovery (MLDv1) for IPv6
- RFC3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC4601: Protocol Independent Multicast-Sparse Mode (PIM-SM)
- RFC5059: Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
- RFC4607: Source-Specific Multicast for IP

1.2 Configuration Task Summary

The IPv6 multicast route management configuration includes the following tasks:

(1) Configuring Basic Functions of IPv6 Multicast

(2) (Optional) Configuring the Maximum Number of Entries in an IPv6 Multicast Routing Table

(3) (Optional) Configuring an IPv6 Multicast Border

(4) (Optional) Configuring an IPv6 Static Multicast Route

(5) (Optional) Enabling Forced Forwarding of Multicast Packets by Software

(6) (Optional) Enabling L2 Direction Control for Multicast Streams

(7) (Optional) Configuring RPF Route Selection Based on the Longest Match Rule

1.3 Prerequisites

- In the multicast network, all nodes are reachable via IPv6 unicast routes.
- Configuring Basic Functions of IPv6 Multicast.

1.4 Configuring Basic Functions of IPv6 Multicast

1.4.1 Overview

The multicast routing function is enabled in the local network and a PIM network is created to provide data sources and user hosts in the network with the IPv6 multicast service.

A device maintains the routing table used for multicast packet forwarding over an IPv6 multicast routing protocol (for example, PIM-SMv6), and learns information about the status of group members in the directly-connected network segments over the MLDv1/v2 protocol. A host joins a specific IPv6 multicast group by sending an MLD REPORT message.

1.4.2 Restrictions and Guidelines

- The IPv6 multicast routing function should be enabled on each multicast device.
- The IPv6 multicast routing function is enabled prior to different IPv6 multicast protocols.
- The IPv6 multicast routing function and the MLD Snooping function are mutually exclusive.

- The IPv6 multicast protocol function must be enabled on each interface in the multicast network.
- After L3 multicast is enabled in the private VLAN and super VLAN and a multicast source exists in a sub VLAN, an extra entry whose ingress is the sub VLAN into which the multicast stream enters must be copied due to the validity check during multicast forwarding. This increases a multicast hardware entry and decreases the multicast capacity by one.

1.4.3 Prerequisites

In the multicast network, all nodes are reachable via IPv6 unicast routes.

1.4.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IPv6 multicast routing function.

ipv6 multicast-routing

The IPv6 multicast routing function is disabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure an IPv6 multicast protocol.

ipv6 pim sparse-mode

No IPv6 multicast protocol is enabled by default.

1.5 Configuring the Maximum Number of Entries in an IPv6 Multicast Routing Table

1.5.1 Overview

Every multicast data packet received by a device is used to maintain relevant IPv6 multicast routing entries. However, excessive multicast routing entries may exhaust device memory and cause device performance to decrease. Users can restrict the number of entries in the IPv6 multicast routing table based on the actual networking conditions and service performance requirements.

1.5.2 Restrictions and Guidelines

Due to limitations by hardware resources, routing entries that exceed the range permitted by hardware can be forwarded only by software, which causes performance to decrease.

1.5.3 Prerequisites

Configuring Basic Functions of IPv6 Multicast.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of entries in an IPv6 multicast routing table.

ipv6 multicast route-limit *limit* [*threshold*]

By default, a maximum of 4000 entries can be added to an IPv6 multicast routing table.

The configured value of *threshold* must be smaller than or equal to the configured value of *limit*.

1.6 Configuring an IPv6 Multicast Border

1.6.1 Overview

An IPv6 multicast border is configured to define the transmission range of multicast packets. When a multicast border is configured on an interface, this interface cannot forward or receive multicast packets, including those sent from the local host.

1.6.2 Restrictions and Guidelines

- The ACL referenced in this command can be a standard ACL or an extended ACL. If an extended ACL is used, only destination addresses need to be matched.
- This command can be used to filter MLD and PIM-SMv6 protocol packets relevant to the IPv6 multicast group range. Multicast data streams are not sent or received by this multicast border interface.

1.6.3 Prerequisites

- Configuring Basic Functions of IPv6 Multicast.
- Before an IPv6 multicast border is configured, ensure that the corresponding ACL is created and a multicast group range is specified. For details about ACL configuration, see *Configuring ACL*.

1.6.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the IPv6 multicast routing function.

ipv6 multicast boundary *acl-name* [**in** | **out**]

No IPv6 multicast border is configured by default.

1.7 Configuring an IPv6 Static Multicast Route

1.7.1 Overview

An IPv6 static multicast route is configured to specify an RPF interface or RPF neighbor for multicast packets from a specific multicast source. This function is used to modify and connect RPF routes.

- Modify an RPF route. A device expects to receive multicast packets from a source through a specified interface. However, the RPF check result indicates that the RPF interface is not this specified interface. In this case, you need to configure an IPv6 static multicast route to specify this interface as an RPF interface. Upon receiving multicast packets from the source, the device performs RPF check. If the RPF check result indicates that the RPF interface is not this specified interface, the route fails the RPF check.
- Connect an RPF route. If the unicast route is interrupted, the RPF routing fails. In this case, you can configure a static multicast route to specify the RPF interface to complete the RPF check and implement multicast packet forwarding.

1.7.2 Restrictions and Guidelines

To specify an outbound interface rather than a next-hop IP address for the IPv6 static multicast route, ensure that the outbound interface is of the point-to-point type.

1.7.3 Prerequisites

Configuring Basic Functions of IPv6 Multicast.

1.7.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an IPv6 static multicast route.

ipv6 mroute *ipv6-address/prefix-length* [*protocol*] { *ipv6-rpf-addrress* | *interface-type interface-number* } [*distance*]

No IPv6 static multicast route is configured by default.

1.8 Enabling Forced Forwarding of Multicast Packets by Software

1.8.1 Overview

After this function is enabled, all IPv6 multicast data packets destined for the CPU are forcedly forwarded by software.

1.8.2 Restrictions and Guidelines

The cache mechanism and forwarding performance problem may cause packet disorder if the multicast streams are heavy. You are not advised to run this command generally.

1.8.3 Prerequisites

Configuring Basic Functions of IPv6 Multicast.

1.8.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of forced forwarding of multicast packets by software.

msf6 force-forwarding

The function of forced forwarding of IPv6 multicast packets (destined for the CPU) by software is disabled by default.

1.9 Enabling L2 Direction Control for Multicast Streams

1.9.1 Overview

L2 direction control is enabled for multicast streams to control the forwarding of multicast streams on an interface. Multiple commands can be configured for a specified multicast stream so that the stream can be forwarded by multiple interfaces. After direction control is enabled for a multicast stream, the stream can be forwarded only by these configured interfaces. Other interfaces are not permitted to forward the stream.

1.9.2 Restrictions and Guidelines

This function controls only the forwarding of multicast streams on interfaces, but does not directly affect the processing of multicast protocols on the protocol packets. Some features (for example, establishment of L3 hardware forwarding entry) of multicast protocols (such as PIM-SMv6) are driven by multicast data streams, and therefore, the behavior of the multicast routing protocols may still be affected.

1.9.3 Prerequisites

Configuring Basic Functions of IPv6 Multicast.

1.9.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable L2 direction control for multicast streams.

ipv6 multicast static *ipv6-source-address ipv6-group-address interface-type interface-number*

L2 direction control is disabled for multicast streams by default.

1.10 Configuring RPF Route Selection Based on the Longest Match Rule

1.10.1 Overview

In multicast routing, various routing entries, such as static multicast routing entry, MBGP routing entry and unicast routing entry, may exist. If RPF route selection based on the longest match rule is configured, the route with the longest match mask is selected from the optimal routes of multiple routing entries as the RPF route. If the routes have the same mask length, the route with the highest priority is selected from the optimal routes. If they have the same priority, the RPF route is selected in the order of static multicast route, MBGP route, and unicast route.

1.10.2 Restrictions and Guidelines

It is recommended that RPF route selection based on the longest match rule be configured on each device unless otherwise specified.

1.10.3 Prerequisites

Configuring Basic Functions of IPv6 Multicast.

1.10.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure RPF route selection based on the longest match rule.

ipv6 multicast rpf longest-match

By default, the route with the highest priority is selected as the RPF route. If the routes have the same priority, the RPF route is selected in the order of IPv6 static multicast route, IPv6 MBGP route and IPv6 unicast route.

1.11 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

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

Table 1-2 Monitoring

Command	Purpose
clear ipv6 mroute { ***** | *ipv6-group-address* [*ipv6-source –address*] }	Clears the IPv4 hardware forwarding entry.
clear ipv6 mroute statistics { ***** | *ipv6-group-address* [*ipv6-source-address*] }	Clears the statistics about the IPv6 hardware forwarding entry.
show ipv6 mroute [*ipv6-group-or-source-address* [*ipv6-group-or-source-address*]] [**sparse**] [**summary** | **count**]	Displays the IPv6 hardware forwarding entry.
show ipv6 rpf *ipv6-source-address*	Displays the RPF information of a specified IPv6 source address.
show ipv6 mroute static	Displays the IPv6 static multicast route information.
show ipv6 mvif [*interface-type interface-number*]	Displays information about the configured IPv6 multicast interface that takes effect.
show ipv6 mrf6 mfc	Displays the IPv6 L3 hardware forwarding entry.
show msf6 msc	Displays the IPv6 L2 and L3 hardware forwarding entry.
debug nsm mcast6 all	Displays the running procedure of the multicast core.
debug nsm mcast6 fib-msg	Displays the communication procedure between the IPv6 multicast core and protocol module.
debug nsm mcast6 mif	Displays the interface running procedure of the IPv6 multicast core.
debug nsm mcast6 stats	Displays the procedure for processing interfaces and behavior statistics of the IPv6 multicast core.
debug ipv6 mrf forwarding	Displays the procedure for IPv6 L3 multicast forwarding.
debug ipv6 mrf mfc	Displays the procedure for operating IPv6 L3 hardware forwarding entries.
debug ipv6 mrf event	Displays the procedure for processing IPv6 L3 multicast forwarding events.
debug msf6 forwarding	Displays the procedure for IPv6 L2 and L3 multicast packet forwarding.

Command	Purpose
debug msf6 mfc	Displays the procedure for operating IPv6 L2 and L3 hardware forwarding entries.
debug msf6 ssp	Displays the bottom-layer hardware processing procedure of IPv6 L2 and L3 multicast forwarding.
debug msf6 api	Displays the procedure for invoking API interfaces for IPv6 L2 and L3 multicast forwarding.
debug msf6 event	Displays the procedure for processing IPv6 L2 and L3 multicast forwarding events.

1.12 Configuration Examples

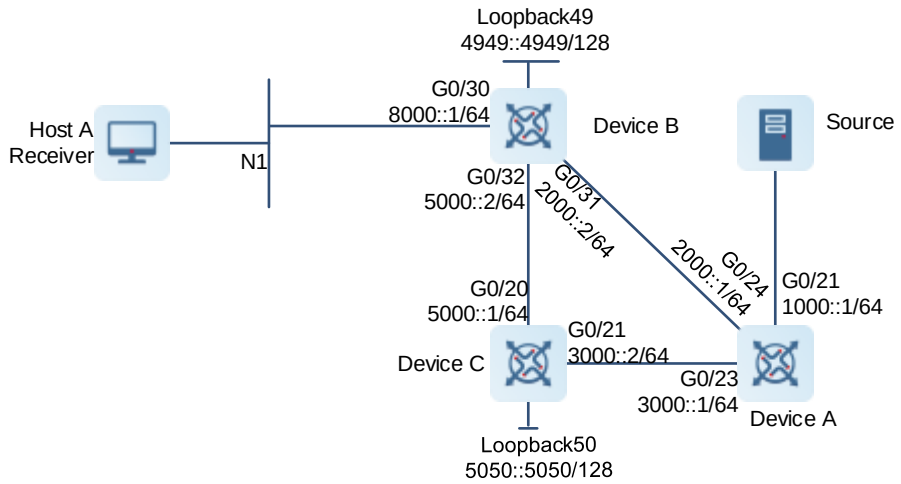
1.12.1 Configuring an IPv6 Static Multicast Route to Modify the RPF Route

1. Requirements

As shown in Figure 1-3, Device A, Device B, and Device C run the OSPF protocol and the PIM-SMv6 function is enabled on each interface. Originally, multicast data sent by the multicast source to Host A is forwarded through the path Device A > Device B. To reduce the load of the link from Device A to Device B, multicast data stream is separated from the unicast data stream. Therefore, the multicast data from the multicast source is sent through the path Device A > Device C > Device B.

2. Topology

Figure 1-3 Topology of IPv6 Static Multicast Route Configuration for Modifying the RPF Route



3. Notes

As shown in Figure 1-3, separate multicast data from unicast data by configuring a static multicast route on Device B to modify the RPF interface of the multicast data. Unicast data is forwarded through the path Device

A > Device B, and multicast data is forwarded through the path Device A > Device C > Device B. The specific configuration method is as follows:

- Configure an IPv6 address and a unicast routing protocol on the multicast devices. A reachable unicast route is a basis of multicast protocol running.
- Enable the IPv6 multicast routing function on all multicast devices. Enable the PIM-SMv6 function on the interfaces connecting multicast devices, the interfaces connecting user hosts, and the multicast source interfaces. Configure C-BSR and C-RP on Device C.
- Configure an RPF static multicast route on Device B, specify Device C as an RPF neighbor, and modify the forwarding path of the multicast data packets.

4. Procedure

(1) Configure an IPv6 address and a unicast routing protocol on the multicast devices.

Configure an IPv6 address and a unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# config terminal
DeviceA(config)# interface GigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# no switchport
DeviceA(config-if-GigabitEthernet 0/21)# ipv6 address 1000::1/64
DeviceA(config-if-GigabitEthernet 0/21)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/21)# exit
DeviceA(config)# interface GigabitEthernet 0/23
DeviceA(config-if-GigabitEthernet 0/23)# no switchport
DeviceA(config-if-GigabitEthernet 0/23)# ipv6 address 3000::1/64
DeviceA(config-if-GigabitEthernet 0/23)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/23)# exit
DeviceA(config)# interface GigabitEthernet 0/24
DeviceA(config-if-GigabitEthernet 0/24)# no switchport
DeviceA(config-if-GigabitEthernet 0/24)# ipv6 address 2000::1/64
DeviceA(config-if-GigabitEthernet 0/24)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/24)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/24)# exit
DeviceA(config)# ipv6 router ospf 4949
```

Configure an IPv6 address and a unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# config terminal
DeviceB(config)# interface GigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# no switchport
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 address 8000::1/64
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 ospf 4949 area 0
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface GigabitEthernet 0/31
DeviceB(config-if-GigabitEthernet 0/31)# no switchport
DeviceB(config-if-GigabitEthernet 0/31)# ipv6 address 2000::2/64
DeviceB(config-if-GigabitEthernet 0/31)# ipv6 ospf 4949 area 0
```

```
DeviceB(config-if-GigabitEthernet 0/31)# exit
DeviceB(config)# interface GigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# no switchport
DeviceB(config-if-GigabitEthernet 0/32)# ipv6 address 5000::2/64
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface Loopback 49
DeviceB(config-if-Loopback 49)# ipv6 address 4949::4949/128
DeviceB(config-if-Loopback 49)# ipv6 ospf 4949 area 0
DeviceB(config-if-Loopback 49)# exit
DeviceB(config)# ipv6 router ospf 4949
```

Configure an IPv6 address and a unicast routing protocol on Device C.

```
DeviceC> enable
DeviceC# config terminal
DeviceC(config)# interface GigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# no switchport
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 address 5000::1/64
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# no switchport
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 address 3000::2/64
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface Loopback 50
DeviceC(config-if-Loopback 50)# ipv6 address 5050::5050/128
DeviceC(config-if-Loopback 50)# ipv6 ospf 4949 area 0
DeviceC(config-if-Loopback 50)# exit
DeviceC(config)# ipv6 router ospf 4949
```

(2) Enable the IPv6 multicast routing function on all multicast devices. Enable the PIM-SMv6 function on the interfaces connecting multicast devices, the interfaces connecting user hosts, and the multicast source interfaces. Configure C-BSR and C-RP on Device C.

Enable the multicast routing and PIM-SMv6 related functions on Device A.

```
DeviceA> enable
DeviceA# config terminal
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/21)# exit
DeviceA(config)# interface GigabitEthernet 0/23
DeviceA(config-if-GigabitEthernet 0/23)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/23)# exit
DeviceA(config)# interface GigabitEthernet 0/24
DeviceA(config-if-GigabitEthernet 0/24)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/24)# exit
```

Enable the multicast routing and PIM-SMv6 related functions on Device B.

```
DeviceB> enable
DeviceB# config terminal
DeviceB(config)# ipv6 multicast-routing
DeviceB(config)# interface GigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface GigabitEthernet 0/31
DeviceB(config-if-GigabitEthernet 0/31)# ipv6 pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/31)# exit
DeviceB(config)# interface GigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# ipv6 pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface Loopback 49
DeviceB(config-if-Loopback 49)# ipv6 pim sparse-mode
DeviceB(config-if-Loopback 49)# exit
```

Enable the multicast routing and PIM-SMv6 related functions on Device C.

```
DeviceC> enable
DeviceC# config terminal
DeviceC(config)# ipv6 multicast-routing
DeviceC(config)# ipv6 multicast-routing
DeviceC(config)# interface GigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface Loopback 50
DeviceC(config-if-Loopback 50)# ipv6 pim sparse-mode
DeviceC(config-if-Loopback 50)# exit
```

Configure C-BSR and C-RP on Device A.

```
DeviceA> enable
DeviceA# config terminal
DeviceA(config)# ipv6 pim bsr-candidate GigabitEthernet 0/21
DeviceA(config)# ipv6 pim rp-candidate GigabitEthernet 0/21
```

(3) Configure an RPF static multicast route on Device B, specify Device C as an RPF neighbor, and modify the forwarding path of the multicast data packets.

```
DeviceB> enable
DeviceB# config terminal
DeviceB(config)# ipv6  mroute 1000::/64 5000::1
```

5. Verification

(1) Run the **show ipv6 mld groups** command on Device B to check whether Host A joins the group FF15::11 and the multicast source 1000::2 sends packets to the group FF15::11.

```
DeviceB> enable
```

```
DeviceB# show ipv6 mld groups
MLD Connected Group Membership
Group Address                        Interface                        Uptime
Expires   Last Reporter
ff15::11                            GigabitEthernet 0/30              00:12:17
00:03:00  fe80::8205:88ff:fe22:b468
DeviceB#
```

(2) Run the **show ipv6 mroute** command on Device A to display the hardware forwarding entry and check whether the next hop is Device C and the outbound interface is GigabitEthernet 0/23.

```
DeviceA> enable
DeviceA# show ipv6 mroute

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed,
      R - RPT, S - SPT, s - SSM Group
Timers: Uptime/Stat Expiry
Interface State: Interface

(1000::2, ff15::11), uptime 00:08:53, stat expires 00:03:12
Owner PIMSMV6, Flags: TFS
  Incoming interface: GigabitEthernet 0/21
  Outgoing interface list:
    GigabitEthernet 0/23

DeviceA#
```

(3) Run the **show ipv6 rpf** command on Device B to check whether the next hop of the multicast source is Device C and the RPF interface is GigabitEthernet 0/32.

```
DeviceB# show ipv6 rpf 1000::
RPF information for 1000::
RPF interface: GigabitEthernet 0/32
  RPF neighbor: 5000::1
  RPF route: 1000::/64
  RPF type: static
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
Distance: 0
  Metric: 0
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
```

```
interface GigabitEthernet 0/21
 no switchport
 ipv6 address 1000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/23
 no switchport
 ipv6 address 3000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/24
 no switchport
 ipv6 address 2000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim bsr-candidate GigabitEthernet 0/21
ipv6 pim rp-candidate GigabitEthernet 0/21
!
```

- Device B configuration file

```
hostname DeviceB
!
ipv6 multicast-routing
!
ipv6 mroute 1000::/64 5000::1
!
interface GigabitEthernet 0/30
 no switchport
 ipv6 address 8000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/31
 no switchport
 ipv6 address 2000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/32
 no switchport
 ipv6 address 5000::2/64
```

```
 ipv6 pim sparse-mode
!
interface Loopback 49
 ipv6 address 4949::4949/128
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
```

- Device C configuration file

```
hostname DeviceC
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/20
 no switchport
 ipv6 address 5000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/21
 no switchport
 ipv6 address 3000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface Loopback 50
 ipv6 address 5050::5050/128
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
```

7. Common Errors

- IPv6 unicast routing is incorrectly configured.
- The IPv6 multicast routing function is not enabled on a multicast device.
- No IPv6 multicast protocol is enabled on an interface.

1.12.2 Configuring a Static Multicast Route to Connect the RPF Route

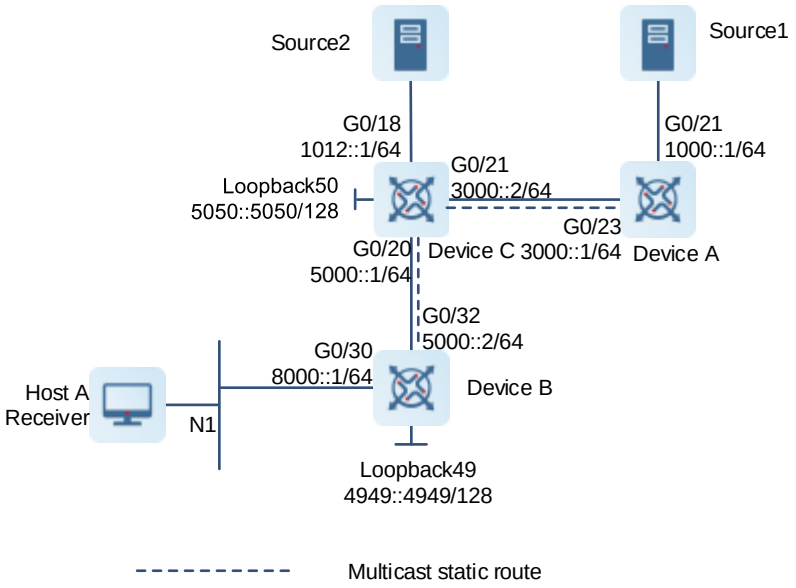
1. Requirements

As shown in Figure 1-4, Device B and Device C run the OSPF protocol, and the unicast route to Device A is isolated. The PIM-SMv6 function is enabled on the interfaces of Device A, Device B and Device C. Host A can

normally receive multicast data packets from Source 2, and it is required to receive multicast data packets from Source 1 as well.

2. Topology

Figure 1-4 Topology of IPv6 Static Multicast Route Configuration for Connecting the RPF Route



3. Notes

Configure a static multicast route to establish an RPF route that is destined to source 1 based on the path Device B > Device C > Device A. The specific configuration method is as follows:

- Configure an IPv6 address for each interface of the devices, and configure the OSPF protocol on Device B and Device C to separate multicast routes from unicast routes on Device A.
- Enable the IPv6 multicast routing function, configure the PIM-SMv6 protocol on each L3 interface of the devices and configure the C-BSR and C-RP in the global configuration, and enable the MLD function on the interface connected to hosts.
- Configure static multicast routes to source 1 on Device B and Device C.

4. Procedure

(1) Configure an IPv6 address for each interface of the devices, and configure the OSPF protocol on Device B and Device C to separate multicast routes from unicast routes on Device A.

Configure an IPv6 address for the interface on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# no switchport
DeviceA(config-if-GigabitEthernet 0/21)# ipv6 address 1000::1/64
DeviceA(config-if-GigabitEthernet 0/21)# exit
DeviceA(config)# interface GigabitEthernet 0/23
```

```
DeviceA(config-if-GigabitEthernet 0/23)# no switchport
DeviceA(config-if-GigabitEthernet 0/23)# ipv6 address 3000::1/64
DeviceA(config-if-GigabitEthernet 0/23)# exit
DeviceA(config)# ipv6 route 5050::5050/128 3000::2
```

Configure an IPv6 address and the OSPF protocol for the interface on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface GigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# no switchport
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 address 8000::1/64
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 ospf 4949 area 0
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface GigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# no switchport
DeviceB(config-if-GigabitEthernet 0/32)# ipv6 address 5000::2/64
DeviceB(config-if-GigabitEthernet 0/32)# ipv6 ospf 4949 area 0
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface Loopback 49
DeviceB(config-if-Loopback 49)# ipv6 address 4949::4949/128
DeviceB(config-if-Loopback 49)# ipv6 ospf 4949 area 0
DeviceB(config-if-Loopback 49)# exit
DeviceB(config)# ipv6 router ospf 4949
DeviceB(config-router)# exit
```

Configure an IPv6 address and the OSPF protocol for the interface on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# interface GigabitEthernet 0/18
DeviceC(config-if-GigabitEthernet 0/18)# no switchport
DeviceC(config-if-GigabitEthernet 0/18)# ipv6 address 1012::1/64
DeviceC(config-if-GigabitEthernet 0/18)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/18)# exit
DeviceC(config)# interface GigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# no switchport
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 address 5000::1/64
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# no switchport
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 address 3000::2/64
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface Loopback 50
DeviceC(config-if-Loopback 50)# ipv6 address 5050::5050/128
DeviceC(config-if-Loopback 50)# ipv6 ospf 4949 area 0
DeviceC(config-if-Loopback 50)# exit
```

```
DeviceC(config)# ipv6 router ospf 4949
DeviceC(config-router)# exit
```

(2) Enable the IPv6 multicast routing function, configure the PIM-SMv6 protocol on each L3 interface of the devices and configure the C-BSR and C-RP in the global configuration, and enable the MLD function on the interface connected to hosts.

Enable the IPv6 multicast routing function and configure the PIM-SMv6 protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/21)# exit
DeviceA(config)# interface GigabitEthernet 0/23
DeviceA(config-if-GigabitEthernet 0/23)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/23)# exit
```

Enable the IPv6 multicast routing function and configure the PIM-SMv6 protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 multicast-routing
DeviceB(config)# interface GigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface GigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# ipv6 pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface Loopback 49
DeviceB(config-if-Loopback 49)# ipv6 pim sparse-mode
DeviceB(config-if-Loopback 49)# exit
```

Enable the IPv6 multicast routing function and functions related to the PIM-SMv6 protocol on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# ipv6 multicast-routing
DeviceC(config)# interface GigabitEthernet 0/18
DeviceC(config-if-GigabitEthernet 0/18)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/18)# exit
DeviceC(config)# interface GigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface Loopback 50
DeviceC(config-if-Loopback 50)# ipv6 pim sparse-mode
DeviceC(config-if-Loopback 50)# exit
```

```
DeviceC(config)# ipv6 pim bsr-candidate Loopback 50
DeviceC(config)# ipv6 pim rp-candidate Loopback 50
```

Enable Source 1 (1000::2/64) and Source 2 (1012::2/64) to send multicast data packets to the multicast group (FF14::10). Add Host A to the multicast group (FF14::10) so that Host A can receive multicast data packets from Source 2 but cannot receive multicast data packets from Source 1.

Run the **show ipv6 rpf** 1000::2 command on Device C. No route exists. No RPF route to Source 1 exists on Device C.

(3) Configure static multicast routes to source 1 on Device B and Device C.

On Device B, configure an RPF static multicast route and configure Device C as an RPF neighbor to Source 1.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mroute 1000::/64 5000::1
```

On Device C, configure an RPF static multicast route and configure Device A as an RPF neighbor to Source 1.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# ipv6 mroute 1000::/64 3000::1
```

5. Verification

Run the **show ipv6 rpf** 1000::2 command on Device B to display the RPF information of Source 1. The RPF information is displayed as follows:

```
DeviceB> enable
DeviceB# show ipv6 rpf 1000::2
RPF information for 1000::2
RPF interface: GigabitEthernet 0/32
  RPF neighbor: 5000::1
  RPF route: 1000::/64
  RPF type: static
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
Distance: 0
  Metric: 0
DeviceB#
```

Run the **show ipv6 rpf** 1000::2 command on Device C to display the RPF information of Source 1. The RPF information is displayed as follows:

```
DeviceC> enable
DeviceC# show ipv6 rpf 1000::2
RPF information for 1000::2
RPF interface: GigabitEthernet 0/21
  RPF neighbor: 3000::1
  RPF route: 1000::/64
  RPF type: static
```

```
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
Distance: 0
  Metric: 0
DeviceC#
```

Enable Source 1 and Source 2 to send multicast data packets to the multicast group (FF14::10), and add Host A to the multicast group.

Run the **show ipv6 pim sparse-mode mroute** command on Device B and Device C to display routing entry information. The multicast entries of Source 1 exist on Device B and Device C. Host A normally receives multicast data packets from Source 1.

```
DeviceC> enable
DeviceC# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 2
(S,G,rpt) Entries: 2
FCR Entries: 0
REG Entries: 0

(*, ff14::10)
RP: 5050::5050
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
```

```
0 . . .
j . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
FCR:

(1000::2, ff14::10)
RPF nbr: fe80::2d0:f8ff:fe22:358d
RPF idx: GigabitEthernet 0/21
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 11 seconds
kat expires in 209 seconds
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
```

```
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
```

```
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

(1000::2, ff14::10, rpt)
RP: 5050::5050
RPF nbr: ::
RPF idx: None
Upstream State: PRUNED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
Pruned
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

(1012::2, ff14::10)
RPF nbr: fe80::2d0:f8ff:fe22:363d
RPF idx: GigabitEthernet 0/18
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 19 seconds
kat expires in 147 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
```

```
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
```

```
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

(1012::2, ff14::10, rpt)
RP: 5050::5050
RPF nbr: ::
RPF idx: None
Upstream State: PRUNED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
Pruned
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Outgoing
0 . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .

DeviceC#

DeviceB> enable
DeviceB# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 2
REG Entries: 0
```

```
(*, ff14::10)
RP: 5050::5050
RPF nbr: fe80::274:9cff:feee:f49f
RPF idx: GigabitEthernet 0/32
Upstream State: JOINED
jt_timer expires in 58 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .
i  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
0  .
j  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Asserted
```

```
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
FCR:
Source: 1000::2
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Outgoing
0 .
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
 KAT timer running, 120 seconds remaining
 Packet count 1
Source: 1012::2
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Outgoing
```

```
0  .
0  . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  .
1  . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2  . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3  . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4  . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5  . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6  . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7  . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
 KAT timer running, 99 seconds remaining
 Packet count 1

DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/21
 no switchport
 ipv6 address 1000::1/64
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/23
 no switchport
 ipv6 address 3000::1/64
 ipv6 pim sparse-mode
!
ipv6 route 5050::5050/128 3000::2
!
```

- Device B configuration file

```
hostname DeviceB
!
ipv6 multicast-routing
!
```

```
ipv6 mroute 1000::/64 5000::1
!
interface GigabitEthernet 0/30
 no switchport
 ipv6 address 8000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/32
 no switchport
 ipv6 address 5000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
```

- Device C configuration file

```
hostname DeviceC
!
ipv6 multicast-routing
!
ipv6 mroute 1000::/64 3000::1
!
interface GigabitEthernet 0/18
 no switchport
 ipv6 address 1012::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/20
 no switchport
 ipv6 address 5000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/21
 no switchport
 ipv6 address 3000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface Loopback 50
 ipv6 address 5050::5050/128
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
```

```
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim bsr-candidate Loopback 50
ipv6 pim rp-candidate Loopback 50
!
```

7. Common Errors

- IPv6 unicast routing is incorrectly configured.

Contents

1 Configuring MLD 1
1.1 Introduction 1
1.1.2 Working Principles of MLDv1 2
1.1.3 Working Principles of MLDv2 6
1.1.4 MLD SSM Mapping 7
1.1.5 MLD Proxy 7
1.1.6 Protocols and Standards 8
1.2 Restrictions and Guidelines 8
1.3 Configuration Task Summary 8
1.4 Prerequisites 9
1.5 Configuring Basic Functions of MLD 9
1.5.1 Overview 9
1.5.2 Restrictions and Guidelines 9
1.5.3 Prerequisites 9
1.5.4 Procedure 9
1.6 Configuring an MLD Version 10
1.6.1 Overview 10
1.6.2 Restrictions and Guidelines 10
1.6.3 Prerequisites 10
1.6.4 Procedure 10
1.7 Enabling Security Control for MLD Multicast 11
1.7.1 Overview 11

1.7.2 Configuration Tasks 11

1.7.3 Prerequisites 11

1.7.4 Enabling Access Control for Multicast Groups 11

1.7.5 Configuring the Maximum Number of Group Members 12

1.8 Configuring MLD Querier Parameters 13

1.8.1 Overview 13

1.8.2 Restrictions and Guidelines 13

1.8.3 Prerequisites 13

1.8.4 Configuration Tasks 13

1.8.5 Configuring the Last Member Query Interval 13

1.8.6 Configuring the Last Member Query Times 14

1.8.7 Configuring the General Group Query Interval 15

1.8.8 Configuring the Maximum Response Time of Query Packets 15

1.8.9 Configuring the Other Querier Keepalive Time 16

1.8.10 Configuring the Robustness Variable of the MLD Querier 16

1.9 Configuring Static MLD Groups 17

1.9.1 Overview 17

1.9.2 Restrictions and Guidelines 17

1.9.3 Prerequisites 17

1.9.4 Procedure 17

1.10 Configuring a Device Interface as a Simulated Host to Join a Group 17

1.10.1 Overview 17

1.10.2 Restrictions and Guidelines 18

1.10.3 Prerequisites 18

1.10.4 Procedure....18

1.11 Enabling the MLD Proxy Function....18

1.11.1 Overview....18

1.11.2 Restrictions and Guidelines....18

1.11.3 Prerequisites....18

1.11.4 Procedure....18

1.12 Enabling the SSM Mapping Function....19

1.12.1 Overview....19

1.12.2 Restrictions and Guidelines....19

1.12.3 Prerequisites....19

1.12.4 Procedure....19

1.13 Monitoring....20

1.14 Examples....21

1.14.1 Configuring Basic Functions of MLD....21

1.14.2 Configuring the MLD Proxy Function....29

1.14.3 Configuring SSM Mapping....33

1.15 Common Misconfigurations....37

1.15.1 What Can I Do when On-demand Multicast Service Is Unavailable on Client....37

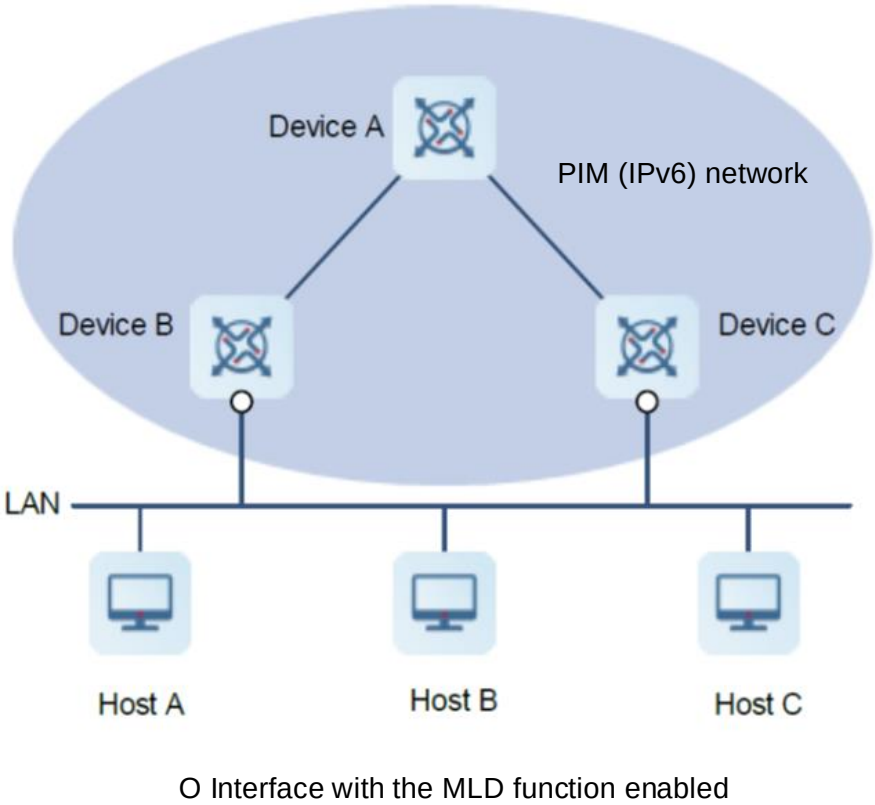
1 Configuring MLD

1.1 Introduction

The Multicast Listener Discovery (MLD) protocol manages IPv6 multicast members.

MLD defines how to establish and maintain membership between multicast devices and member hosts in an IPv6 network, to decide a forwarding path of multicast streams. Figure 1-1 shows the topology of MLD in an IPv6 multicast network.

Figure 1-1 Topology of MLD in a Multicast Network



There are two versions of MLD: MLDv1 is based on version 2 of the Internet Group Management Protocol (IGMP) and MLDv2 is based on version 3 of IGMP. A later MLD version is backward-compatible with an earlier MLD version. MLDv1 completes IPv6 member management based on the query and report mechanism. MLDv2 supports member hosts to decide whether to receive packets from a specified multicast source on the basis of MLDv1.

- MLD of both versions supports the Any-Source Multicast (ASM) model.
- MLDv2 can be directly applied to the Source-Specific Multicast (SSM) model.
- MLDv1 can be applied to the SSM model only when MLD SSM mapping is configured.

1.1.2 Working Principles of MLDv1

The querier election mechanism, general group query and report mechanism, join mechanism, and leave mechanism are defined in MLDv1.

1. Types of MLDv1 Packets

MLDv1 supports the following four types of packets:

- General group query packet: A querier sends general group query packets to all multicast devices and hosts in the same network segment to understand groups with members.
- Group-specific query packet: A querier sends query packets to specified multicast groups in the same network segment to understand whether these groups contain members.
- Report packet: A host sends report packets to the querier to respond to the query packets or join a group.
- Leave packet: A host sends leave packets to the querier when the host leaves a group, notifying the querier that it leaves the specified group.

2. Working Mechanisms of MLDv1

- Querier election

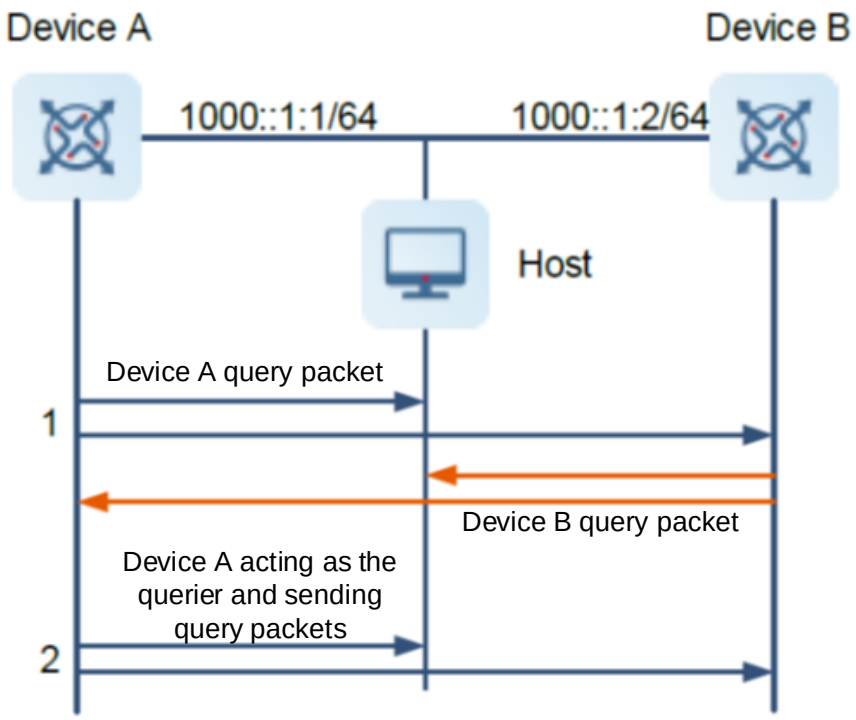
  If multiple multicast devices exist in a network segment, only one multicast device needs to send query packets as a querier. This avoids redundancy. When the querier in the network segment fails, other devices in the same network segment need to take the role and process MLD protocol packets. During querier election, interface addresses of the devices are compared. The device with a smallest IP address is elected as the querier, as shown in Figure 1-2.

  a Device A and Device B consider themselves as the querier and send query packets to the local network segment.

  b They compare the source IPv6 address in the received packets with the address of their interfaces. The address of Device A is smaller. Therefore, Device A acts as the querier to periodically send query packets.

  c Device B fails in the election and starts a query keepalive timer. When the timer expires, Device B considers that the querier fails and starts to send query packets to initiate a new round of querier election.

Figure 1-2 Querier Election Diagram



- General group query and report

  The MLD querier periodically sends general group query packets to all hosts and multicast devices in the local network segment, and understands and maintains group membership based on the report packets replied by the member hosts. Figure 1-3 shows the general group query and report procedure.

  a The MLD querier Device A periodically sends general group query packets to the destination address FF02::1.

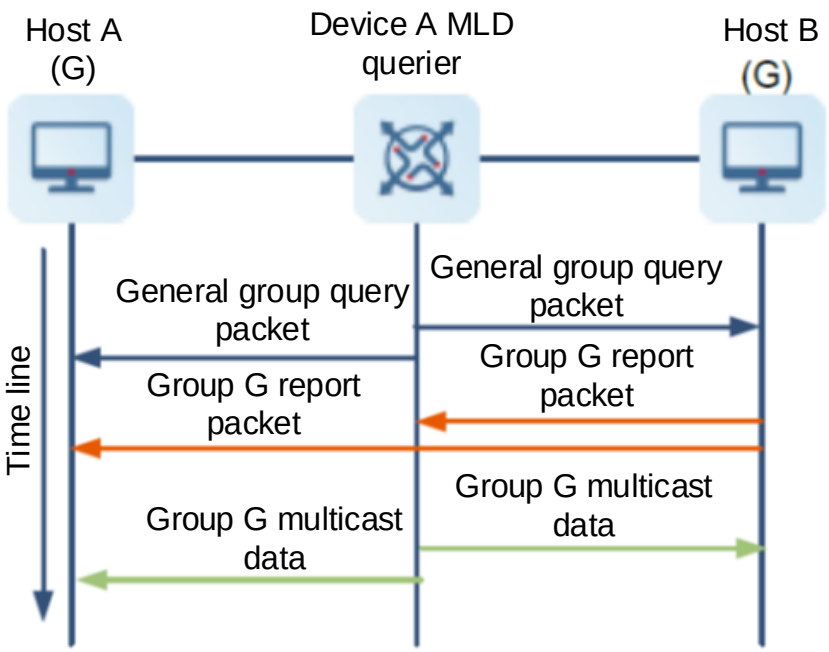
  d Upon receiving the general group query packets, Host A and Host B in the multicast group G start respective timers Timer-G-A and Timer-G-B.

  e The host whose timer expires first sends report packets destined for the multicast group G.

  If the timer Timer-G-A of Host A expires first, Host A sends report packets to the multicast group G. Upon receiving the report packets, Host B stops its timer and sends report packets in the network segment.

  f Upon receiving the report packets destined for the multicast group G from Host A, the MLD querier knows that there is member in the multicast group G. The multicast routing protocol generates an (*, G) entry. Upon receiving multicast data destined for the multicast group G, the MLD querier forwards the multicast data in the network segment.

Figure 1-3 General Group Query and Report Diagram



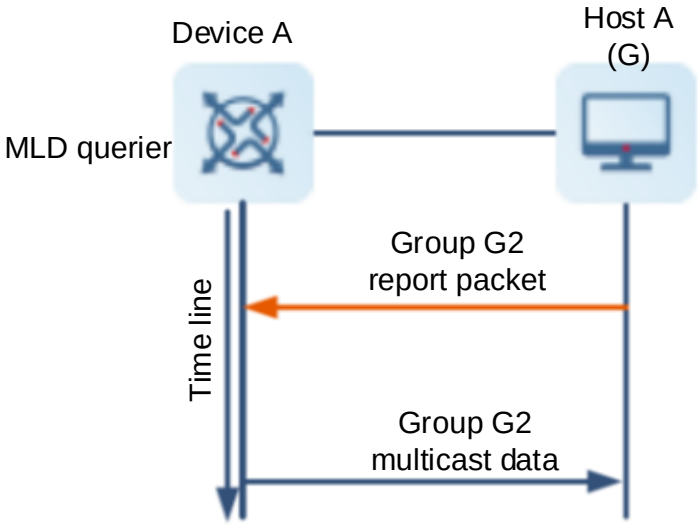
- Member join

  When a host tries to join a multicast group, it takes some time for the host to join the group if the host waits for a general group query packet from the querier and replies a report packet. If the host can proactively send a report packet to the MLD querier, the querier can immediately generate a multicast forwarding entry upon receiving the packet. If multicast devices in the group receive multicast data, the new host can quickly get multicast service. Figure 1-4 shows the new member join procedure.

  a Before receiving a general group query packet from Device A, Host A proactively sends a report packet destined for the multicast group G, to notify that Host A joins the multicast group G.

  g Upon receiving the report packet, the MLD querier Device A knows that there is a member in the multicast group G in the current network segment. The multicast routing protocol generates an (*, G) entry. Upon receiving multicast data destined for the multicast group G, the MLD querier forwards the multicast data in the network segment.

Figure 1-4 Member Join Diagram



- Member leave

  Upon receiving a leave packet from a member to plan to leave the multicast group G, the MLD querier sends a group-specific query packet to understand whether there is any other member existing in the group in the network segment. If not, the MLD querier deletes the corresponding membership to reduce redundant multicast traffic in the network and save bandwidth. Figure 1-5 shows the member leave procedure.

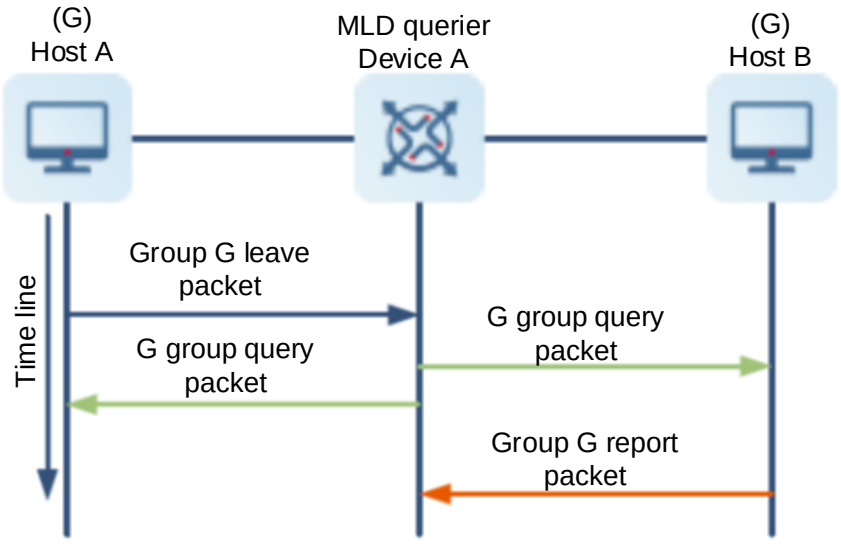
  a Host A sends a leave packet destined for all multicast devices in the local network segment to leave the multicast group G.

  h Upon receiving the leave packet, the MLD querier Device A sends a group-specific query packet destined for the multicast group G.

  i If there is any other member (for example, Host B) in the multicast group G, Host B sends a report packet for the multicast group G upon receiving the query packet. The MLD querier continues to maintain the membership of the multicast group G upon receiving the report packet. The (*, G) entry remains existent. Upon receiving multicast data destined for the multicast group G, the MLD querier forwards the multicast data in the network segment.

  j If there is no other member in the multicast group G, the querier receives no report packet for the multicast group G. After the timer expires, the (*, G) entry is deleted. Upon receiving multicast data destined for the multicast group G, the MLD querier does not forward the multicast data in the network segment.

Figure 1-5 Member Leave Diagram



1.1.3 Working Principles of MLDv2

1. Changes of MLDv2 from MLDv1

- In MLDv2, when you add a host to a group, you can specify the host to receive multicast data from specified sources. In MLDv1, you cannot specify sources for a host.
- In MLDv1, an MLDv1 packet can carry information of only one multicast group. In MLDv2, an MLDv2 packet can carry information of multiple multicast groups. This relieves the interaction problem of a great number of packets between hosts and the querier.

2. Types of MLDV2 Packets

- Query packets include general group query packet, group-specific query packet, and source-specific query packet (check whether members in a group receive multicast data from the specific source).
- Member report packets include multicast group and multicast source information. A source can be filtered in INCLUDE or EXCLUDE mode. (G, INCLUDE, (S1, S2...)) means to receive multicast data sent only from specified sources S1, S2, ... to the group G. (G, EXCLUDE, (S1, S2...)) means to reject multicast data sent from specified sources S1, S2, ... to the group G.

3. Working Mechanisms of MLDv2

Compared with MLDv1, MLDv2 supports you to select sources for a host to receive multicast data when you add the host.

- Specify sources to receive multicast data: You can specify sources for the host to receive multicast data when you add the host to a multicast group.
- Query a specified source: Upon receiving a report packet to modify the correspondence between multicast sources and groups from members, the MLD querier sends a specified source query packet. If you expect a member to receive multicast data from a specified source, configure a report packet. The MLD querier updates the source list of this group based on the report.

1.1.4 MLD SSM Mapping

In the source-specific multicast (SSM) model, a host must run MLDv2 if you want to specify source addresses for the host. If a host supports only MLDv1, a multicast source cannot be specified for the host. To enable a host that supports only MLDv1 to use the SSM service, you can enable the MLD SSM mapping function on the multicast device.

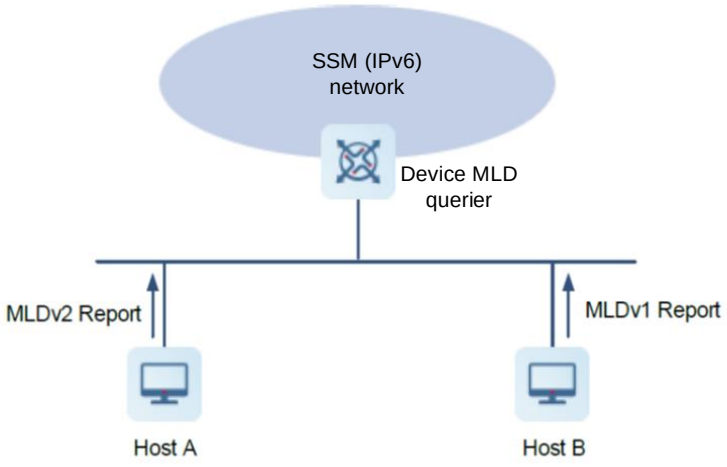
Based on the MLD SSM mapping mechanism, static SSM address mapping rules can be configured on the multicast device to convert the (*, G) information in MLDv1 report packets to (S, G) information so that the SSM service can be used by the host that supports only MLDv1.

In the SSM network shown in Figure 1-6, the MLD multicast device runs MLDv2, Host A supports only MLDv1, and Host B supports MLDv2. The MLD SSM mapping function can be enabled on the MLD querier to provide SSM service for Host A.

In this network, when the device receives an MLDv1 report packet from Host A, the device checks the address of the IPv6 multicast group G in the packet.

- If the multicast group G is not in the IPv6 SSM group address range, the ASM service is provided.
- If the multicast group G is in the IPv6 SSM group address range, whether the ASM service can be provided depends on the following situation:
  - If no MLD SSM mapping rule is configured on the device for the multicast group G, the SSM service cannot be provided and the packet is discarded.
  - If an MLD SSM mapping rule is configured on the device for the multicast group G, the (*, G) information in the MLDv1 report packet is mapped to (G, INCLUDE, (S1, S2)) and the SSM multicast service is provided.

Figure 1-6 Topology of MLD SSM Mapping



1.1.5 MLD Proxy

In some user scenarios, if you do not want devices connected to hosts to run complete multicast routing protocols, you can enable the MLD proxy function.

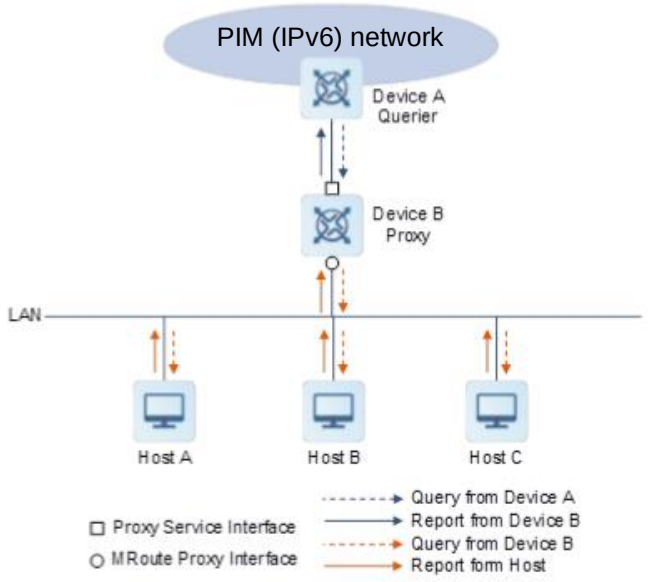
On the user side, the MLD proxy acts as a querier and periodically queries user information. On the route side, the MLD proxy acts a host and sends user information to a network when necessary. In this way, L2 multicast

flooding is suppressed, user information is more effectively obtained and controlled, and the protocol packets and network load are reduced to some extent.

Two types of MLD proxy interfaces are defined to facilitate understanding:

- MLD proxy service interface: This interface is responsible for behaviors of hosts. It receives query packets from uplink devices, replies report packets based on current group membership, and sends report or leave packets when the membership changes.
- MLD MRoute proxy interface: This interface is responsible for behaviors of the querier. It sends query packets, collects host information, and maintains membership.

Figure 1-7 Topology of MLD Proxy



1.1.6 Protocols and Standards

- RFC2710: Multicast Listener Discovery (MLDv1) for IPv6
- RFC3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6

1.2 Restrictions and Guidelines

- In an IPv6 network, all L3 devices must run the IPv6 PIM protocol before multicast forwarding entries can be established normally.
- Device interfaces must run MLDv2 before hosts supporting either MLD version can use the SSM service.
- A member host can be a PC or a set top box (STB), and it can normally receive multicast data by the multicast client software.

1.3 Configuration Task Summary

MLD configuration includes the following tasks:

(1) Configuring Basic Functions of MLD

(2) (Optional) Configuring an MLD Version

(3) Enabling Security Control for MLD Multicast. All the configuration tasks below are optional. Select the configuration tasks as required.

- Enabling Access Control for Multicast Groups
- Configuring the Maximum Number of Group Members

(4) Configuring MLD Querier Parameters. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Last Member Query Interval
- Configuring the Last Member Query Times
- Configuring the General Group Query Interval
- Configuring the Maximum Response Time of Query Packets
- Configuring the Other Querier Keepalive Time
- Configuring the Robustness Variable of the MLD Querier

(5) (Optional) Configuring Static MLD Groups

(6) (Optional) Configuring a Device Interface as a Simulated Host to Join a Group

(7) (Optional) Enabling the MLD Proxy Function

(8) (Optional) Enabling the SSM Mapping Function

1.4 Prerequisites

An IPv6 unicast routing protocol is configured to ensure that device nodes are reachable through IPv6 unicast routes.

1.5 Configuring Basic Functions of MLD

1.5.1 Overview

The multicast routing function is enabled on the local network and group information on the local network is collected so that member hosts can join multicast groups to receive multicast data packets.

1.5.2 Restrictions and Guidelines

- The IPv6 multicast routing function should be enabled on each multicast device on the local network unless otherwise specified.
- The PIM-SMv6 function should be enabled on an L3 interface directly connected to the local network unless otherwise specified.

1.5.3 Prerequisites

All PIM interfaces should be reachable through IPv6 unicast routes.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IPv6 multicast routing function.

ipv6 multicast-routing

The IPv6 multicast routing function is disabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

PIM interfaces must be L3 interfaces, including routing, L3AP, SVI, and loopback interfaces.

(5) Enable the PIM-SMv6 function.

ipv6 pim sparse-mode

The PIM-SMv6 function on an interface is disabled by default.

1.6 Configuring an MLD Version

1.6.1 Overview

At present, there are two versions of MLD. Multicast devices running MLDv2 can identify MLDv1 packets. Multicast devices running MLDv1 cannot identify MLDv2 packets.

1.6.2 Restrictions and Guidelines

- After an MLD version is configured, MLD automatically restarts.
- The MLD version on a multicast device must be later than or equal to the MLD version on a host.
- It is recommended that an MLD version be configured on all multicast device interfaces directly connected to the local network unless otherwise specified.

1.6.3 Prerequisites

Configuring Basic Functions of MLD.

1.6.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an MLD version.

ipv6 mld version { **1** | **2** }

MLDv2 is running on an interface by default.

1.7 Enabling Security Control for MLD Multicast

1.7.1 Overview

- To prevent a host from joining an IPv6 multicast group, you can enable the function of filtering the MLD group on the interface directly connected to a network segment.
- To prevent a great number of hosts from joining an IPv6 multicast group and affecting interface performance of devices, you can configure the maximum number of members on the interface directly connected to a network segment.
- To prevent a great number of hosts from joining an IPv6 multicast group and affecting the overall performance of devices, you can configure the maximum number of members on the devices.

1.7.2 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Enabling Access Control for Multicast Groups
- Configuring the Maximum Number of Group Members

1.7.3 Prerequisites

Configuring Basic Functions of MLD.

1.7.4 Enabling Access Control for Multicast Groups

1. Overview

After enabling access control for multicast groups on an interface, you can control hosts from joining groups in the directly connected network segment. ACLs are used to limit the group address range. Report packets denied by the ACLs are discarded.

When MLDv2 is enabled, this command supports extended ACLs to precisely filter source record information in MLDv2 packets. If the received MLD report packets follow the format of (S1, S2, S3, ..., Sn, G), the corresponding ACL must be configured for filtering. S1, S2, S3, ..., Sn correspond to source addresses in ACL entries, and G corresponds to the destination address in the ACL entries.

2. Restrictions and Guidelines

It is recommended that access control be enabled on all multicast device interfaces directly connected to the local network unless otherwise specified.

3. Prerequisites

Before a multicast group address range is configured, ensure that the corresponding ACL is created and a multicast group range is specified. For details about ACL configuration, see *Configuring ACL*.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

PIM interfaces must be L3 interfaces, including routing, L3AP, SVI, and loopback interfaces.

(4) Enable access control for multicast groups.

ipv6 mld access-group *acl-name*

An interface allows hosts to join any group by default.

1.7.5 Configuring the Maximum Number of Group Members

1. Overview

To prevent a great number of hosts from joining an IPv6 multicast group, you can limit the number of members.

- In the global configuration mode, the number of members in an MLD group on a device is limited.
- In the interface configuration mode, the number of members in an MLD group on an interface is limited.

If the number of group members exceeds the interface limit or global limit, subsequent report packets are ignored.

If an exceptional list is configured, report packets in a specified range can be normally processed, and the records about these group members are not counted.

Interface and global limits can be configured separately. If the global limit is smaller than the interface limit, the global limit prevails.

2. Restrictions and Guidelines

It is recommended that the maximum number of group members be configured on all multicast device interfaces directly connected to the local network unless otherwise specified.

It is recommended that the maximum number of group members be configured on multicast devices directly connected to the local network unless otherwise specified.

3. Prerequisites

- Before an exceptional list is configured, ensure that the corresponding ACL is created and an exceptional multicast group range is specified. For details about ACL configuration, see *Configuring ACL*.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of MLD group members. Select one of the following to configure.

- Configure the maximum number of MLD group members on a device.

  ipv6 mld limit *limit* [**except** *acl-name*]

- Configure the maximum number of MLD group members on an interface.

  interface *interface-type interface-number*

  ipv6 mld limit *limit* [**except** *acl-name*]

By default, the maximum number of MLD group members on a device is **64000**, and that on an interface is **4000**.

1.8 Configuring MLD Querier Parameters

1.8.1 Overview

MLD maintains IPv6 membership by query packets and report packets. If multiple multicast devices exist in a network segment, only one multicast device needs to send query packets as a querier. IP addresses of multicast devices are compared. The device with the smallest address is elected as the querier. The querier periodically sends query packets to obtain local member information and ensure that a group has at least one host. If no host is available in a group, the group is deleted by the device.

The MLD querier work can be adjusted using multiple parameters. When the default parameter values are used, the querier can normally work. Network optimization can be implemented by adjusting querier parameter values to avoid excessive protocol packets and network congestion. Also, membership can be updated and maintained in time.

1.8.2 Restrictions and Guidelines

- It is recommended that querier parameters be configured on all multicast device interfaces directly connected to the local network unless otherwise specified.
- In actual network deployment, to accurately, timely, and stably maintain group membership and avoid non-queriers from initiating a new round of election, ensure that the following durations are arranged in ascending order: Maximum response time of general group query packet < Sending interval of general group query packet < Other querier keepalive time.

1.8.3 Prerequisites

Configuring Basic Functions of MLD.

1.8.4 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Last Member Query Interval
- Configuring the Last Member Query Times
- Configuring the General Group Query Interval
- Configuring the Maximum Response Time of Query Packets
- Configuring the Robustness Variable of the MLD Querier
- Configuring the Other Querier Keepalive Time

1.8.5 Configuring the Last Member Query Interval

1. Overview

Before a host leaves a multicast group, the host sends a leave packet. Upon receiving the leave packet, the querier continuously sends group-specific/source-specific query packets and waits for responses from hosts. This parameter specifies the query packet sending interval.

2. Restrictions and Guidelines

- It is recommended that this parameter be configured on all multicast device interfaces directly connected to the local network unless otherwise specified.
- The unit of the last member query interval is 0.1 seconds. If the parameter value is 10, the actual sending interval is 1 second.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the last member query interval.

ipv6 mld last-member-query-interval *interval*

The group-specific query packet sending interval is **1** second by default.

1.8.6 Configuring the Last Member Query Times

1. Overview

Before a host leaves a multicast group, the host sends a leave packet. Upon receiving the leave packet, the querier continuously sends specific group/source query packets and waits for responses from the host. This parameter specifies the query packet sending times.

2. Restrictions and Guidelines

It is recommended that this parameter be configured on all multicast device interfaces directly connected to the local network unless otherwise specified.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the last member query times.

ipv6 mld last-member-query-count *count*

The group-specific query packet sending times is **2** by default.

1.8.7 Configuring the General Group Query Interval

1. Overview

The MLD querier periodically sends query packets to all hosts and multicast devices on the shared network. This parameter specifies the interval for sending query packets.

2. Restrictions and Guidelines

It is recommended that this parameter be configured on all multicast device interfaces directly connected to the local network unless otherwise specified.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the general group query interval.

ipv6 mld query-interval *interval*

The default interval for sending general group query packets is **125** seconds.

1.8.8 Configuring the Maximum Response Time of Query Packets

1. Overview

After the MLD querier sends query packets, member hosts reply upon receiving the query packets before the maximum response time expires. If no response is received after timeout, it is considered that no member exists in the group of the directly connected network segment and the group information is deleted.

2. Restrictions and Guidelines

It is recommended that this parameter be configured on all multicast device interfaces directly connected to the local network unless otherwise specified.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum response time of query packets.

ipv6 mld query-max-response-time *max-response-time*

The maximum response time of query packets is **10** seconds by default.

1.8.9 Configuring the Other Querier Keepalive Time

1. Overview

When a non-querier does not receive a query packet in the same network segment within a specified period, the non-querier considers there is only querier (itself) in the directly connected network segment and initiates a new round of querier election. This parameter specifies the timeout time for the non-queriers to wait for query packets.

2. Restrictions and Guidelines

It is recommended that this parameter be configured on all interfaces where MLD is enabled on the local network unless otherwise specified.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the other querier keepalive time.

ipv6 mld querier-timeout *timeout*

The keepalive time of other querier is **255** seconds by default.

1.8.10 Configuring the Robustness Variable of the MLD Querier

1. Overview

When the query packets sent by the querier are lost due to network instability, the query packets are retransmitted. The retransmission times are referred to as the robustness variable of the MLD querier.

In the event of packet loss, query packet retransmission occurs in either of the following situations:

- When the querier is started, it sends general group query packets.
- Upon receiving leave packets, the querier sends group-specific/source-specific query packets to check whether there are members existing in the specific multicast group.

2. Restrictions and Guidelines

It is recommended that this parameter be configured on all interfaces where MLD is enabled on the local network unless otherwise specified.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the robustness variable of the MLD querier.

ipv6 mld robustness-variable *robustness*

The robustness variable of the MLD querier is **2** by default.

1.9 Configuring Static MLD Groups

1.9.1 Overview

In some application scenarios, a static multicast group may need to be configured on the interfaces connected to group members in the following cases:

1. The group members are stable and multicast data needs to be quickly and stably forwarded to member interfaces.
2. The group members cannot send report packets but need to receive certain multicast data. After the static multicast group is configured, the multicast devices consider that group members exist on these interfaces and forward multicast data to these interfaces.

1.9.2 Restrictions and Guidelines

A static multicast group must be manually configured on an interface connected to group members.

1.9.3 Prerequisites

Configuring Basic Functions of MLD.

1.9.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a static MLD group.

ipv6 mld static-group *ipv6-group-address*

No interface is added to any static multicast group by default.

1.10 Configuring a Device Interface as a Simulated Host to Join a Group

1.10.1 Overview

In some test scenarios, no host is available or can be added to a multicast group. In this case, you need to configure device interfaces to simulate hosts and add the hosts to a specific multicast group.

1.10.2 Restrictions and Guidelines

- Only L3 interfaces can be configured as hosts.
- An interface can be added to multiple groups at the same time.

1.10.3 Prerequisites

The PIM protocol must be configured and the IPv6 multicast routing function must be enabled on the interfaces to be configured as hosts.

1.10.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a device interface as a host to join a group.

ipv6 mld join-group *ipv6-group-address*

No interface is added to any multicast group by default.

1.11 Enabling the MLD Proxy Function

1.11.1 Overview

The MLD router proxy function collects local member information. For a host, the MLD proxy functions as a router and sends query packets.

For the querier, the MLD proxy functions as a host and sends report packets.

1.11.2 Restrictions and Guidelines

- The MLD proxy service interface is configured on the interface of routers directly connected to the upstream devices unless otherwise specified.
- The MRoute proxy interface is configured on the interface of hosts directly connected to the downstream devices unless otherwise specified.
- A maximum of 32 proxy service interfaces can be configured on a device. After receiving MLD query packets, the proxy service interface sends report packets based on the MLD group member records.

1.11.3 Prerequisites

Configuring Basic Functions of MLD.

1.11.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the MLD proxy service function.

ipv6 mld proxy-service

The MLD proxy service function is disabled by default.

(5) Enable the MLD MRoute proxy function.

ipv6 mld mroute-proxy *interface-type interface-number*

The MRoute proxy function is disabled by default.

1.12 Enabling the SSM Mapping Function

1.12.1 Overview

MLDv2 supports source filtering while MLDv1 does not. However, the multicast devices provide the SSM mapping function to implement source filtering and enable MLDv1 hosts to use the SSM service. Multicast device interfaces run MLDv2. When receiving MLDv1 report packets, a multicast device adds the static mapping source address.

1.12.2 Restrictions and Guidelines

The SSM service must be enabled and the SSM group address range must be consistent on all multicast devices.

1.12.3 Prerequisites

- Configuring Basic Functions of MLD.
- Before a static mapping entry is configured, ensure that the corresponding ACL is created and a multicast group range is specified. For details about ACL configuration, see *Configuring ACL*.

1.12.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the SSM mapping function.

ipv6 mld ssm-map enable

The SSM mapping function is disabled by default.

(4) (Optional) Configure a static mapping entry.

ipv6 mld ssm-map static *acl-name ipv6-source-address*

No static mapping entry is configured by default.

1.13 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear ipv6 mld group [*ipv6-group-address*] [*interface-type interface-number*]	Clears dynamic group member records in the MLD cache.
clear ipv6 mld interface *interface-type interface-number*	Clears all MLD statistics and group member records on the interface.
show ipv6 mld groups [*ipv6-group-address* | *interface-type interface-number*] [**detail**]	Displays groups directly connected to the device and group information learned from MLD.
show ipv6 mld interface [*interface-type interface-number*]	Displays configurations of the interface.
show ipv6 mld ssm-mapping [*ipv6-group-address*]	Displays the SSM mapping information.
show debugging	Displays the MLD debugging switch status.
debug ipv6 mld all	Debugs all MLD information.
debug ipv6 mld decode	Debugs MLD packet resolution.
debug ipv6 mld encode	Debugs MLD packet encoding.
debug ipv6 mld events	Debugs MLD event information.
debug ipv6 mld fsm	Debugs MLD event information.
debug ipv6 mld tib	Debugs MLD state machine information.
debug ipv6 mld warning	Debugs MLD alarms.

1.14 Examples

1.14.1 Configuring Basic Functions of MLD

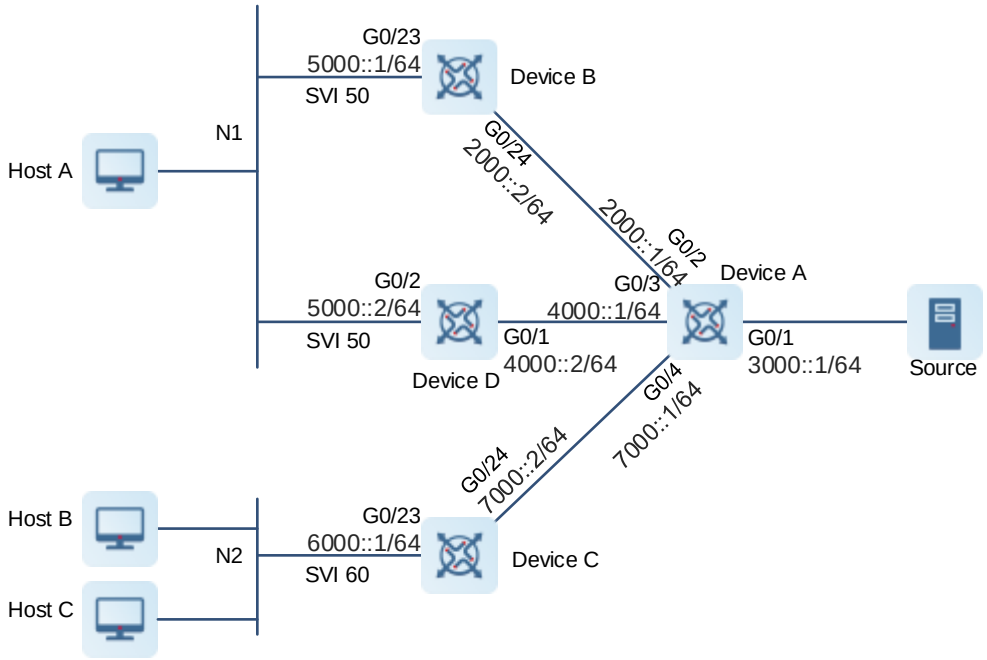
1. Requirements

As shown in Figure 1-8, Host A, Host B, and Host C residing in shared networks N1 and N2 of IPv6 want to receive video information from the source in multicast mode. The static multicast group FF13::1 is configured on N1 shared network, and hosts on N2 shared network can join the multicast group FF14::1.

- OSPFv3 runs in the network to make uniticast routes between any two nodes reachable.
- Device B and Device D are connected to the shared network N1 through SVI 50. The IPv6 address of Device B is smaller than the IPv6 address of Device D. Therefore, Device B acts as the querier, and Host A is the multicast information receiver in the shared network N1.
- Device C is connected to the shared network N2 through SVI 60, and Host B is the multicast information receiver in the shared network N2.
- Device B, Device C, and Device D are connected to other devices in the IPv6 PIM network through L3 interfaces.

2. Topology

Figure 1-8 Topology for Basic Functions of MLD



3. Notes

- Configure an IPv6 unicast routing protocol OSPFv3 on a multicast device and ensure that unicast routes are reachable to the Loopback interface.
- Enable the IPv6 multicast routing function on all multicast devices.
- Configure the PIM-SMv6 protocol on the interconnected interfaces of devices, interfaces connected to hosts, and interfaces connected to sources.

- Configure a static multicast group on the interfaces of the devices on shared network N1.
- Enable the multicast group access control function on the interfaces of the devices on shared network N2.

4. Procedure

(1) Configure an IPv6 address for each interface and configure the unicast routing protocol.

Configure an IPv6 address for the interface of Device A and configure the OSPFv3 protocol to implement internetworking. Perform the same configuration on Device B, Device C, and Device D.

```
DeviceA> enable
DeviceA# config terminal
DeviceA(config)# ipv6 router ospf 5050
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no switchport
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 address 3000::1/64
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 ospf 5050 area 0
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface GigabitEthernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# no switchport
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 address 2000::1/64
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 ospf 5050 area 0
DeviceA(config-if-GigabitEthernet 0/2)# exit
DeviceA(config)# interface GigabitEthernet 0/3
DeviceA(config-if-GigabitEthernet 0/3)# no switchport
DeviceA(config-if-GigabitEthernet 0/3)# ipv6 address 8000::1/64
DeviceA(config-if-GigabitEthernet 0/3)# ipv6 ospf 5050 area 0
DeviceA(config-if-GigabitEthernet 0/3)# exit
DeviceA(config)# interface GigabitEthernet 0/4
DeviceA(config-if-GigabitEthernet 0/4)# no switchport
DeviceA(config-if-GigabitEthernet 0/4)# ipv6 address 7000::1/64
DeviceA(config-if-GigabitEthernet 0/4)# ipv6 ospf 5050 area 0
DeviceA(config-if-GigabitEthernet 0/4)# exit
DeviceA(config)# interface loopback 0
DeviceA(config-if-Loopback 0)# ipv6 address 1111::1/128
DeviceA(config-if-Loopback 0)# ipv6 ospf 5050 area 0
DeviceA(config-if-Loopback 0)# exit
```

(2) Enable the IPv6 multicast routing function on all devices, and configure the PIM-SMv6 protocol on the interconnected interfaces of devices, interfaces connected to hosts, and interfaces connected to sources.

Enable the IPv6 multicast routing function and configure the PIM-SMv6 protocol on Device A. Perform the same configuration on Device B, Device C, and Device D.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface GigabitEthernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

```
DeviceA(config)# interface GigabitEthernet 0/3
DeviceA(config-if-GigabitEthernet 0/3)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/3)# exit
DeviceA(config)# interface GigabitEthernet 0/4
DeviceA(config-if-GigabitEthernet 0/4)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/4)# exit
DeviceA(config)# interface loopback 0
DeviceA(config-if-Loopback 0)# ipv6 pim sparse-mode
DeviceA(config-if-Loopback 0)# exit
```

Configure an RP. Configure a C-BSR and a C-RP on Device A.

```
DeviceA(config)# ipv6 pim bsr-candidate Loopback 0
DeviceA(config)# ipv6 pim rp-candidate Loopback 0
```

(3) Configure a static multicast group on the interfaces of the devices on shared network N1.

Configure a static multicast group on SVI 50 of Device B, and set the static multicast group address to FF13::1. Perform the same configuration on Device D.

```
DeviceB> enable
DeviceB# config terminal
DeviceB(config)# interface VLAN 50
DeviceB (config-if-VLAN 50)# ipv6 mld static-group ff13::1
DeviceB(config-if-VLAN 50)# exit
DeviceB(config)# interface GigabitEthernet 0/23
DeviceB(config-if-GigabitEthernet 0/23)# switchport access vlan 50
DeviceB(config-if-GigabitEthernet 0/23)# exit
DeviceB(config)# interface TenGigabitEthernet 0/27
DeviceB(config-if-TenGigabitEthernet 0/27)# switchport mode trunk
DeviceB(config-if-TenGigabitEthernet 0/27)# switchport trunk native vlan 50
DeviceB(config-if-TenGigabitEthernet 0/27)# exit
```

(4) Enable the multicast group access control function on the interfaces of the devices on shared network N2.

Enable the multicast group access control function on SVI 60 of Device C, and add the hosts in network N2 to the multicast group FF14::1.

```
DeviceC> enable
DeviceC# config terminal
DeviceC(config)# ipv6 access-list ipv6-group
DeviceC(config-ipv6-acl)# permit ipv6 any host FF14::1
DeviceC(config-ipv6-acl)# exit
DeviceC(config)# interface VLAN 60
DeviceC(config-if-VLAN 60)# ipv6 mld access-group ipv6-group
DeviceC(config-if-VLAN 60)# exit
```

5. Verification

Run the **show ipv6 mld interface** command to display MLD configuration of each device. Device B is taken as an example. Device B is the querier, because the IPv6 address of SVI 50 on Device B in the shared network N1 is smaller.

```
DeviceB# show ipv6 mld interface VLAN 50
```

```
Interface VLAN 50 (Index 4146)
 MLD Enabled, Active, Querier, Version 2 (default)
 Internet address is fe80::274:9cff:feee:53cb
 MLD interface limit is 4000
 MLD interface has 0 group-record states
 MLD interface has 0 join-group records
 MLD interface has 1 static-group records
 MLD activity: 10 joins, 1 leaves
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 10 (1/10s)
 Last member query count is 2
 Group Membership interval is 260
 Robustness Variable is 2
```

Run the **show ipv6 pim sparse-mode mroute** command to display the multicast routing entries on each device. The multicast routing entries on Device B are as follows:

```
DeviceB# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
REG Entries: 0

(*, ff13::1)
RP: 1111::1
RPF nbr: fe80::274:9cff:fe11:c9e7
RPF idx: GigabitEthernet 0/24
Upstream State: NOT JOINED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
27 28 29 30 31
Local
0  .i  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
 .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
.  .  .
```

```
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . .
FCR:
```

Run the **show ipv6 mld groups** command to display the static multicast group FF13::1 that SVI50 joins on Device B and Device D.

```
DeviceB# show ipv6 mld groups
MLD Connected Group Membership
Group Address                    Interface         Uptime    Expires   Last
Reporter
ff13::1                         VLAN 50           00:11:07  stopped   ::
```

Try to add a host to the multicast groups FF13::1 and FF14::1 through SVI 60, and run the **show ipv6 mld groups** command to display that the host joins in only the multicast group FF14::1 through SVI 60.

```
DeviceC# show ipv6 mld groups
MLD Connected Group Membership
Group Address                      Interface          Uptime    Expires   Last
Reporter
ff14::1                           VLAN 60            00:01:03  00:03:51
fe80::274:9cff:feee:f49f
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ipv6 address 3000::1/64
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ipv6 address 2000::1/64
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/3
 no switchport
 ipv6 address 4000::1/64
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/4
 no switchport
 ipv6 address 7000::1/64
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface Loopback 0
 ipv6 address 1111::1/128
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 5050
 graceful-restart
```

```
!
ipv6 pim bsr-candidate Loopback 0
ipv6 pim rp-candidate Loopback 0
!
end
```

- Device B configuration file

```
hostname DeviceB
!
ipv6 multicast-routing
!
vlan range 1,50
!
interface GigabitEthernet 0/23
 switchport access vlan 50
!
interface GigabitEthernet 0/24
 no switchport
 ipv6 address 2000::2/64
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface TenGigabitEthernet 0/27
 switchport mode trunk
 switchport trunk native vlan 50
!
interface Loopback 0
 ipv6 address 2222::2/128
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface VLAN 50
 ipv6 address 5000::1/64
 ipv6 ospf 5050 area 0
 ipv6 mld static-group ff13::1
 ipv6 pim sparse-mode
!
ipv6 router ospf 5050
 graceful-restart
!
End
```

- Device C configuration file

```
hostname DeviceC
!
ipv6 access-list ipv6-group
 10 permit ipv6 any host FF14::1
```

```
!
ipv6 multicast-routing
!
vlan range 1,60
!
interface GigabitEthernet 0/23
 switchport access vlan 60
!
interface GigabitEthernet 0/24
 no switchport
 ipv6 address 7000::2/64
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface Loopback 0
 ipv6 address 3333::3/128
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface VLAN 60
 ipv6 address 6000::1/64
 ipv6 mld access-group ipv6-group
 ipv6 mld join-group ff13::1
 ipv6 mld join-group ff14::1
 ipv6 pim sparse-mode
!
ipv6 router ospf 5050
 graceful-restart
!
end
```

- Device D configuration file

```
hostname DeviceD
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ipv6 address 4000::2/64
 ipv6 ospf 5050 area 0
!
interface TenGigabitEthernet 0/51
 switchport mode trunk
 switchport trunk native vlan 50
!
interface Loopback 0
 ipv6 address 4444::4/128
```

```
!
interface VLAN 50
 ipv6 address 5000::2/64
 ipv6 ospf 5050 area 0
 ipv6 mld static-group ff13::1
 ipv6 pim sparse-mode
!
ipv6 router ospf 5050
 graceful-restart
!
end
```

7. Common Errors

- The multicast routing function is not enabled on a multicast device.
- No multicast interface is available on the network.

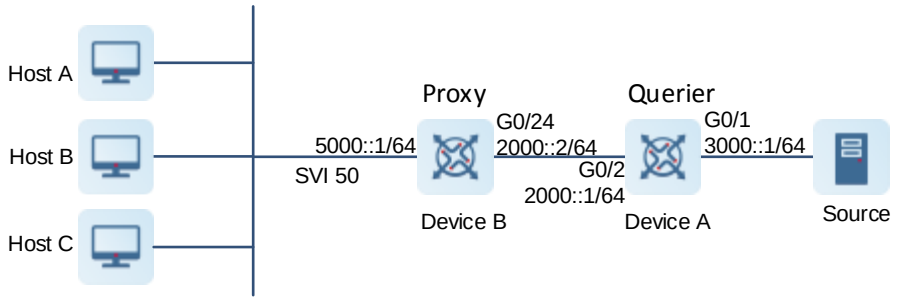
1.14.2 Configuring the MLD Proxy Function

1. Requirements

As shown in Figure 1-9, the PIM-SMv6 protocol is configured in the network. Host A and Host B in the stub network receive multicast data from the source. The multicast group addresses are FF13::1 and FF14::1. The MLD proxy function is enabled on Device B to maintain membership and normal forwarding of multicast data.

2. Topology

Figure 1-9 Topology of the MLD Proxy



3. Notes

- Configure an IPv6 unicast routing protocol OSPFv3 on a multicast device and ensure that unicast routes are reachable to the Loopback interface.
- Enable the IPv6 multicast routing function on all multicast devices, and configure the PIM-SMv6 protocol on the interconnected interfaces of devices, interfaces connected to hosts, and interfaces connected to sources.
- Configure a proxy service interface.
- Configure an MRoute proxy interface.

4. Procedure

(1) Configure an IPv6 unicast routing protocol OSPFv3 on a multicast device and ensure that unicast routes are reachable to the Loopback interface.

Configure an IPv6 address for the interface of Device A and configure the OSPFv3 protocol to implement internetworking. Perform the same configuration on Device B.

```
DeviceA> enable
DeviceA# config terminal
DeviceA(config)# ipv6 router ospf 5050
DeviceA(config)# interface GigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no switchport
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 address 3000::1/64
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 ospf 5050 area 0
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface GigabitEthernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# no switchport
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 address 2000::1/64
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 ospf 5050 area 0
DeviceA(config-if-GigabitEthernet 0/2)# exit
DeviceA(config)# interface loopback 0
DeviceA(config-if-Loopback 0)# ipv6 address 1111::1/128
DeviceA(config-if-Loopback 0)# ipv6 ospf 5050 area 0
DeviceA(config-if-Loopback 0)# exit
```

(2) Enable the IPv6 multicast routing function on all multicast devices, and configure the PIM-SMv6 protocol on the interconnected interfaces of devices, interfaces connected to hosts, and interfaces connected to sources.

Enable the IPv6 multicast routing function and configure the PIM-SMv6 protocol on Device A. Perform the same configuration on Device B.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface GigabitEthernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/2)# exit
DeviceA(config)# interface loopback 0
DeviceA(config-if-Loopback 0)# ipv6 pim sparse-mode
DeviceA(config-if-Loopback 0)# exit
```

Configure an RP. Configure a C-BSR and a C-RP on Device A.

```
DeviceA(config)# ipv6 pim bsr-candidate Loopback 0
DeviceA(config)# ipv6 pim rp-candidate Loopback 0
```

(3) Configure a proxy service interface.

Configure GigabitEthernet 0/24 on Device B as a proxy service interface.

```
DeviceB> enable
```

```
DeviceB# config terminal
DeviceB(config)# interface GigabitEthernet 0/24
DeviceB(config-if-GigabitEthernet 0/24)# ipv6 mld proxy-service
DeviceB(config-if-GigabitEthernet 0/24)# exit
```

(4) Configure an MRoute proxy interface.

Configure SVI 50 of Device B as an MRoute proxy interface.

```
DeviceB(config)# interface VLAN 50
DeviceB(config-if-VLAN 50)# ipv6 mld mroute-proxy GigabitEthernet 0/24
```

5. Verification

Run the **show ipv6 mld groups** command on Device B to display the proxy entries.

```
DeviceB# show ipv6 mld groups
MLD Connected Group Membership
Group Address                        Interface          Uptime    Expires   Last
Reporter
ff13::1                             VLAN 50            00:03:24  00:04:14
fe80::274:9cff:feee:f49f
ff14::1                             VLAN 50            00:00:06  00:04:14
fe80::274:9cff:feee:54cb

MLD Proxy-server Connected Group Membership
Group Address                        Interface             Uptime
ff13::1                             GigabitEthernet 0/24    00:03:24
ff14::1                             GigabitEthernet 0/24    00:00:06
```

Run the **show ipv6 mld groups** command on Device A to display that addresses of members joining the multicast groups FF13::1 and FF14::1 are IPv6 addresses of the Device B proxies.

```
DeviceA# show ipv6 mld groups
MLD Connected Group Membership
Group Address                        Interface          Uptime    Expires   Last
Reporter
ff13::1                             GigabitEthernet 0/2  00:09:56  00:03:44
fe80::274:9cff:feee:53cb
ff14::1                             GigabitEthernet 0/2  00:00:23  00:03:56
fe80::274:9cff:feee:53cb
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ipv6 address 3000::1/64
```

```
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/2
 no switchport
 ipv6 address 2000::1/64
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface Loopback 0
 ipv6 address 1111::1/128
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 5050
 graceful-restart
!
ipv6 pim bsr-candidate Loopback 0
ipv6 pim rp-candidate Loopback 0
!
End
```

- Device B configuration file

```
hostname DeviceB
!
ipv6 multicast-routing
!
vlan range 1,50
!
interface GigabitEthernet 0/23
 switchport access vlan 50
!
interface GigabitEthernet 0/24
 no switchport
 ipv6 address 2000::2/64
 ipv6 ospf 5050 area 0
ipv6 mld proxy-service
 ipv6 pim sparse-mode
!
interface TenGigabitEthernet 0/27
 switchport mode trunk
 switchport trunk native vlan 50
!
interface Loopback 0
 ipv6 address 2222::2/128
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
```

```
!
interface VLAN 50
 ipv6 address 5000::1/64
 ipv6 ospf 5050 area 0
ipv6 mld mroute-proxy GigabitEthernet 0/24
 ipv6 pim sparse-mode
!
ipv6 router ospf 5050
 graceful-restart
!
End
```

7. Common Errors

The basic functions of MLD are not enabled.

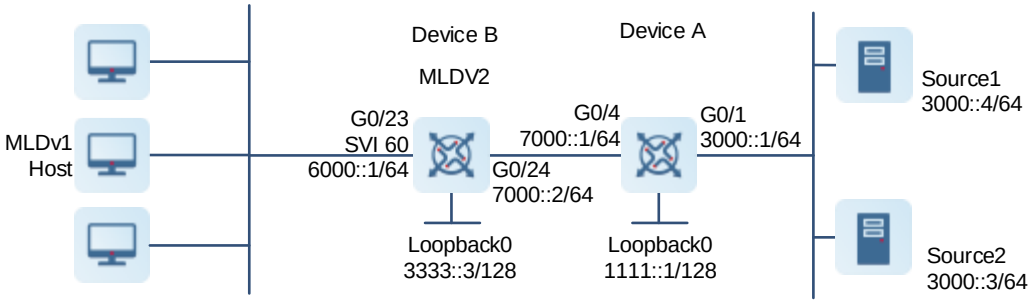
1.14.3 Configuring SSM Mapping

1. Requirements

As shown in Figure 1-10, the SSM model is used to provide multicast service in an IPv6 multicast network. The default SSM group address range in the network is FF3X::/32. Hosts run MLDv1 and do not support MLDv2. Hosts are expected to receive multicast packets from Source 2 and ignore multicast packets from Source 1.

2. Topology

Figure 1-10 Topology of SSM Mapping



3. Notes

- Configure an IPv6 unicast routing protocol OSPFv3 on a multicast device and ensure that unicast routes are reachable to the Loopback interface.
- Enable the IPv6 multicast routing function on all multicast devices, and configure the PIM-SMv6 protocol on the interconnected interfaces of devices, interfaces connected to hosts, and interfaces connected to sources.
- Configure an SSM group address range.
- Enable the SSM mapping function.
- Configure an SSM mapping static linked list.

4. Procedure

(1) Configure an IPv6 unicast routing protocol OSPFv3 on a multicast device and ensure that unicast routes are reachable to the Loopback interface.

Configure an IPv6 address for the interface of Device A and configure the OSPFv3 protocol to implement internetworking. Perform the same configuration on Device B.

```
DeviceA> enable
DeviceA# config terminal
DeviceA(config)# ipv6 router ospf 5050
DeviceA(config)# interface GigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no switchport
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 address 3000::1/64
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 ospf 5050 area 0
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface GigabitEthernet 0/4
DeviceA(config-if-GigabitEthernet 0/4)# no switchport
DeviceA(config-if-GigabitEthernet 0/4)# ipv6 address 7000::1/64
DeviceA(config-if-GigabitEthernet 0/4)# ipv6 ospf 5050 area 0
DeviceA(config-if-GigabitEthernet 0/4)# exit
DeviceA(config)# interface loopback 0
DeviceA(config-if-Loopback 0)# ipv6 address 1111::1/128
DeviceA(config-if-Loopback 0)# ipv6 ospf 5050 area 0
DeviceA(config-if-Loopback 0)# exit
```

(2) Enable the IPv6 multicast routing function on all multicast devices, and configure the PIM-SMv6 protocol on the interconnected interfaces of devices, interfaces connected to hosts, and interfaces connected to sources.

Enable the IPv6 multicast routing function and configure the PIM-SMv6 protocol on Device A. Perform the same configuration on Device B.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface GigabitEthernet 0/4
DeviceA(config-if-GigabitEthernet 0/4)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/4)# exit
DeviceA(config)# interface loopback 0
DeviceA(config-if-Loopback 0)# ipv6 pim sparse-mode
DeviceA(config-if-Loopback 0)# exit
```

Set the MLD version on SVI 60 connected to hosts to 2 on Device B.

```
DeviceB> enable
DeviceB# config terminal
DeviceB(config)# interface VLAN 60
DeviceB(config-if-VLAN 60)# ipv6 mld version 2
DeviceB(config-if-VLAN 60)# exit
```

(3) Configure an SSM group address range.

Configure an SSM multicast address range on all devices. Take Device A as an example and perform the same configuration on Device B.

```
DeviceB(config)# ipv6 pim ssm default
```

(4) Enable the SSM mapping function.

Enable the SSM mapping function on Device B.

```
DeviceB(config)# ipv6 mld ssm-map enable
```

(5) Configure an SSM mapping static linked list.

Map the multicast addresses in FF34::/64 to Source 1 on Device B.

```
DeviceB(config)# ipv6 access-list map-acl
DeviceB(config-ipv6-acl)# permit ipv6 any FF34::/64
DeviceB(config)# ipv6 mld ssm-map static map-acl 3000::3
```

5. Verification

Display the SSM mapping information.

```
DeviceB# show ipv6 mld ssm-mapping
SSM Mapping : Enabled
Database    : Static mappings configured
```

Display multicast source information corresponding to the multicast group FF34::1.

```
DeviceB# show  ipv6 mld ssm-mapping FF34::1
Group address: ff34::1
Database     : Static
Source list  : 3000::3
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ipv6 address 3000::1/64
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/4
 no switchport
 ipv6 address 7000::1/64
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface Loopback 0
 ipv6 address 1111::1/128
```

```
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 5050
 graceful-restart
!
ipv6 pim ssm default
!
end
```

- Device B configuration file

```
hostname DeviceB
!
ipv6 access-list map-acl
 30 permit ipv6 any FF34::/64
!
ipv6 multicast-routing
!
vlan range 1,60
!
interface GigabitEthernet 0/23
 switchport access vlan 60
!
interface GigabitEthernet 0/24
 no switchport
 ipv6 address 7000::2/64
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface Loopback 0
 ipv6 address 3333::3/128
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
!
interface VLAN 60
 ipv6 address 6000::1/64
 ipv6 ospf 5050 area 0
 ipv6 pim sparse-mode
 ipv6 mld version 2
!
ipv6 router ospf 5050
 graceful-restart
!
ipv6 mld ssm-map enable
ipv6 mld ssm-map static map-acl 3000::3
ipv6 pim ssm default
!
```

```
end
```

7. **Common Errors**

- The basic functions of MLD are not enabled.
- The SSM service is not enabled.
- No SSM address range is configured.

1.15 Common Misconfigurations

- Basic functions of MLD are not configured on the proxy service interface.
- No SSM service address is configured when the SSM service is used.
- The SSM service address ranges on different multicast devices are inconsistent.

1.15.1 What Can I Do when On-demand Multicast Service Is Unavailable on Client

- Fault Symptom

  The multicast function is enabled. But I failed to use the on-demand multicast service through a client.

- Troubleshooting

  a Check whether the connection between the on-demand client and multicast server is normal.

  Run the **show ipv6 route** command to check for any entry of unicast route to the multicast source on the server. If no, configure a unicast routing protocol.

  b Check configuration on the devices.

  Run the **show ipv6 pim sparse-mode interface** command to check for PIM information on an interface. If no information about the interface is displayed, the PIM-SMv6 function is not enabled. Run the **ipv6 pim sparse-mode** command to enable the PIM-SMv6 function on the interface.

  c Check whether the multicast receiver normally joins the group.

  Run the **show ipv6 mld groups** command to check whether the host joins the corresponding multicast group on the multicast device residing in the same network segment as the host.

  d Check whether the multicast entries on the multicast source and receiver are normal.

  Run the **show ipv6 pim sparse-mode mroute** command to check whether the multicast entries on the devices are normal.

Contents

1 Configuring PIM-SMv6 1
1.1 Introduction 1
1.2 Principles 1
1.2.1 ASM Model 1
1.2.2 SSM Model 6
1.2.3 Protocols and Standards 7
1.3 Restrictions and Guidelines 8
1.4 Configuration Task Summary 8
1.5 Enabling the PIM-SMv6 Function 8
1.5.1 Overview 8
1.5.2 Restrictions and Guidelines 9
1.5.3 Prerequisites 9
1.5.4 Procedure 9
1.6 Configuring PIM-SMv6 in the ASM Model 9
1.6.1 Overview 9
1.6.2 Configuration Tasks 10
1.6.3 Prerequisites 10
1.6.4 Configuring a Static RP 10
1.6.5 Configuring C-BSRs and Related Parameters 11
1.6.6 Configuring C-RPs and Related Parameters 12
1.6.7 Configuring Registration Parameters 15
1.6.8 Configuring the Last Hop Device to Switch over from the RPT to SPT 18

1.7 Configuring PIM-SMv6 in the SSM Model 18
1.7.1 Overview 18
1.7.2 Restrictions and Guidelines 18
1.7.3 Prerequisites 18
1.7.4 Procedure 19
1.8 Configuring PIM-SMv6 Neighbor Parameters 19
1.8.1 Overview 19
1.8.2 Configuration Tasks 19
1.8.3 Prerequisites 19
1.8.4 Configuring the Neighbor Message Time Parameters 19
1.8.5 Configuring Neighbor Tracking 20
1.8.6 Configuring Neighbor Filtering 20
1.9 Configuring DR Priority 21
1.9.1 Overview 21
1.9.2 Prerequisites 21
1.9.3 Procedure 21
1.10 Configuring Parameters of the Join/Prune Packets 22
1.10.1 Overview 22
1.10.2 Restrictions and Guidelines 22
1.10.3 Configuration Tasks 22
1.10.4 Prerequisites 22
1.10.5 Configuring Join/Prune Packet Sending Interval 22
1.10.6 Configuring the Prune Delay 23
1.11 Enabling PIM-SMv6 BFD Correlation 23

1.12 Monitoring 24

1.13 Configuration Examples..... 25

1.13.1 Configuring Basic Functions of PIM-SMv6 in the ASM Model 25

1.13.2 Configuring Basic Functions of PIM-SMv6 in the SSM Model 53

1 Configuring PIM-SMv6

1.1 Introduction

The Protocol Independent Multicast (PIM) is an intra-domain multicast routing protocol that is independent from unicast routing protocols. Any unicast routing protocol, for example, static route, Routing Information Protocol (RIP), and Open Shortest Path First (OSPF), can provide routing information for IP multicast. Multicast routing is independent of unicast routing, and simply uses unicast routing tables to generate multicast routing information. The Protocol Independent Multicast-Sparse Mode version 6 (PIM-SMv6) is used most widely, and applies to networks of any form, especially large networks where group members are scattered in a wide area. Compared with other intra-domain multicast routing protocols, PIM-SMv6 has irreplaceable advantages.

1.2 Principles

Suppose that not all hosts need to receive multicast data, PIM-SMv6 sends multicast data to hosts that require the multicast data.

A PIM multicast device provides multicast service in any-source multicast (ASM) and source-specific multicast (SSM) models. For groups in the SSM address range, the SSM model is used. For other groups, the ASM model is used. In the ASM model, a host joins a specified multicast group G without the multicast source S specified. In the SSM model, a host can join a specified multicast group G to receive multicast data from a specified source S.

1.2.1 ASM Model

1. Basic Principles

PIM-SMv6 in the ASM model is implemented as follows:

- A rendezvous point (RP) is used as a root of a rendezvous point tree (RPT) for transition. The designated router (DR) connected to a host sends a join message to the RP of a multicast group, and the multicast devices on the route create (*, G) entries hop by hop. Based on the entries, an RPT is created with the RP as the root.
- To send data to a multicast group, the source DR sends a register message to the RP to create an (S, G) entry on the RP. After the registration succeeds, the multicast source sends multicast data to the RP. After the multicast data arrives at the RP, it is copied and sent to the host via the RPT.

In the ASM model, the key mechanisms of PIM-SMv6 include PIM neighbor creation, DR election, RP, bootstrap router (BSR), multicast source registration, shortest path tree (SPT) switchover, and assertion.

2. PIMv6 Neighbor Creation

Neighbor relationship must be created between PIM multicast devices to form a PIM network, so that PIM control messages and multicast packets can be transmitted on the network. A Hello message is sent from a PIM interface. In the multicast packet with the Hello message encapsulated, the destination address is FF02::D (indicating all PIM multicast devices in the same network segment), the source address is the IP address of the PIM interface, and the time to live (TTL) value is 1. The Hello message is used to:

- Discover PIM neighbors.

PIM multicast devices in the same network segment receive the multicast packet with the destination address as FF02::D, obtain neighbor information, and create neighbor relationship. After the neighbor relationship is created, the PIM interfaces can receive and process other PIM packets and create multicast routing entries.

When a PIM interface is enabled or detects a new neighbor, a Triggered-Hello-Delay message is used to generate a random time. Within the time, the interface sends Hello messages.

- Negotiate protocol parameters. The Hello message contains the following key parameters:
  - **DR Priority**: The priority of a multicast device for DR election. The device with a higher priority is selected.
  - **Holdtime**: The neighbor is considered reachable before timeout.
  - **Propagation Delay**: Duration between the time when a PIM device receives a prune packet and the time when the PIM device sends the prune packet to the uplink devices.
  - **Override-Interval**: The interval to override the prune.
- Maintain neighbor relationship.

  A Hello message is sent periodically between PIM multicast devices. If no new Hello message is received from a PIM neighbor within the hold time, this neighbor is considered unreachable and then removed from the neighbor list. Any change of PIM neighbors will cause change of the multicast topology in the network. If an uplink or downlink neighbor in a multicast distribution tree (MDT) is unreachable, multicast routes converge again and the MDT is reshaped.

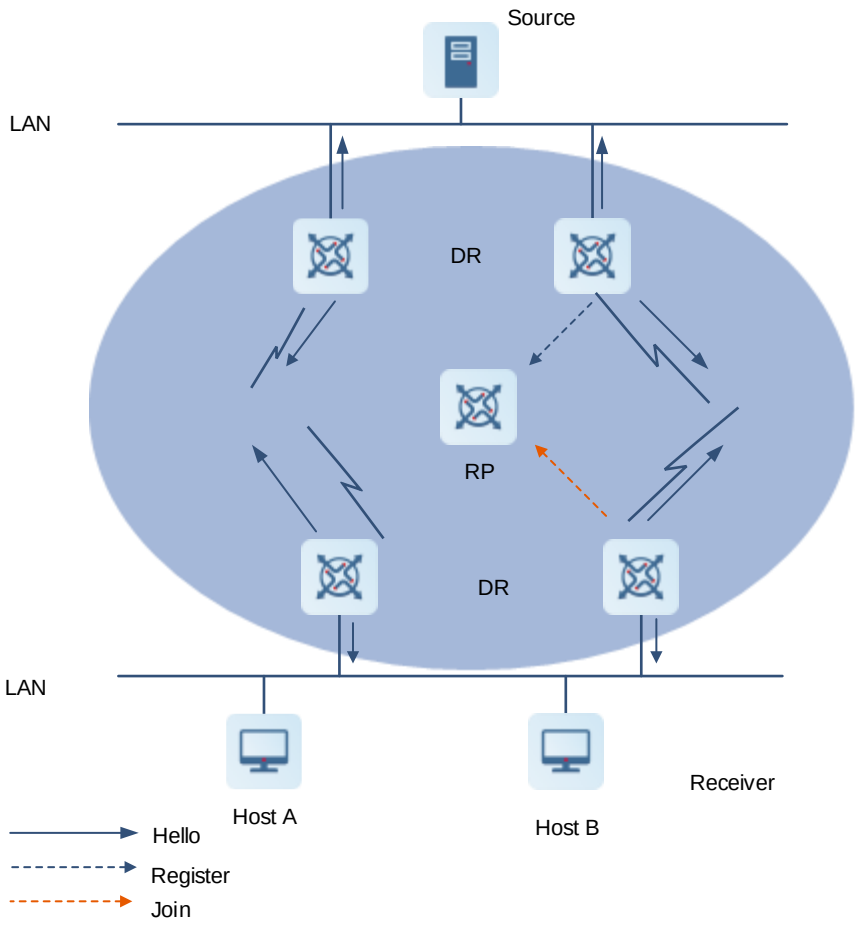
3. DR Election

As shown in Figure 1-1, the source DR sends a register message to the RP. Member DRs send join messages to the RP and forward multicast data to members in a multicast group. In the network segment to which members and multicast source are connected, multiple PIM devices obtain IP addresses and DR priorities of neighbors based on the Hello messages sent between the PIM devices during PIM neighbor creation. The PIM device that is elected becomes a member DR or source DR. The election rules are as follows:

(1) The DR priorities are compared. The device with a higher priority is selected.

(2) If the DR priorities are the same or there is any neighbor in the shared network segment that does not support DR priority, the IP addresses of the devices are compared. The device with a larger IP address is selected.

Figure 1-1 Schematic Diagram of DR Election



4. BSR Election

In the PIM network, the BSR periodically generates bootstrap messages (BSMs) that include a series of candidate-RPs (C-RPs) and corresponding group addresses. The BSMs are sent in the entire domain hop by hop. All PIM multicast devices in the network receive the BSMs and record the C-RPs and corresponding group addresses.

In the PIM-SMv6 domain, one or multiple candidate-BSRs (C-BSRs) are configured and the BSR is elected based on rules.

5. RP Election

In the PIMv6 network, the RP processes register messages of the source DR and join packets of group members. The process from the multicast source to members of the multicast group is divided into two sections: The SPT that uses the source DR as the root and the RP as the leaf, and the RPT that uses the RP as the root and member DRs as leaves. In the PIM-SMv6 network with the ASM model, the RP must act as a transition to create or forward data.

In the PIM network, an RP can serve one or more groups, and a group can be served by only one RP. In the PIM network, the RP can be configured as static or dynamic.

- Static RP

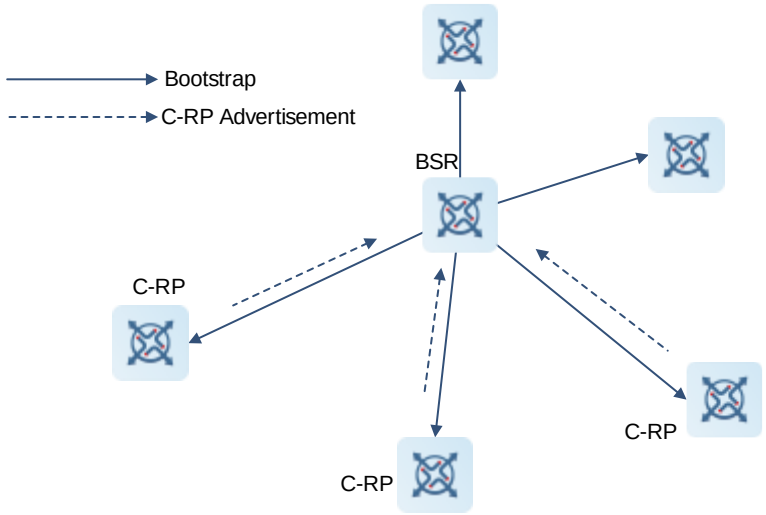
A static RP sets the RP address on each PIM multicast device to enable the entire PIMv6 network to know the RP address.

- Dynamic RP

  Multiple C-RPs can be configured in a PIM-SMv6 domain to elect an RP dynamically. These C-RPs add their own addresses and served multicast groups to advertisement packets and sent the packets to the BSR periodically in unicast mode. The BSR is elected from the configured C-BSRs based on rules. The BSR periodically generates BSMs that include a series of C-RPs and corresponding group addresses. The BSMs are sent in the entire domain. Each PIM device in the domain receives and saves these BSMs, and applies the same hash algorithms to compute and elect an RP for each group.

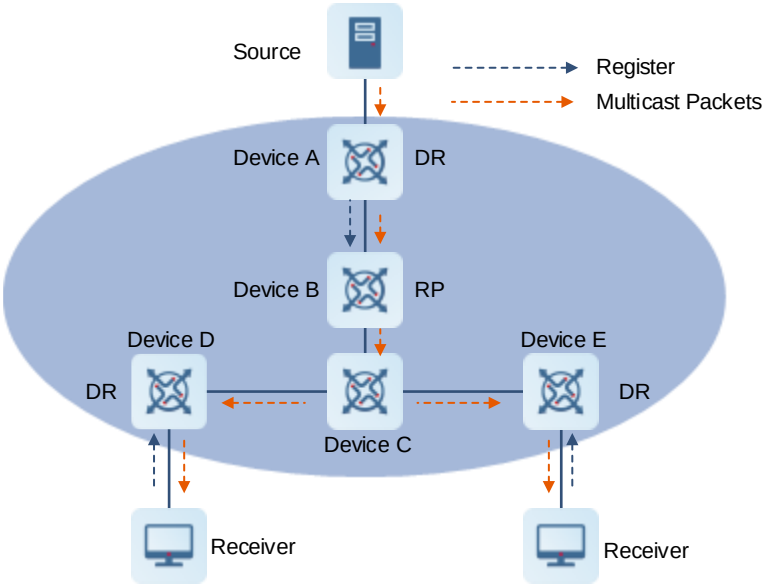
  - BSR election process: Initially, each C-BSR considers itself a BSR and sends a BSM throughout the network. The BSMs carry the C-BSR addresses and priorities. Upon receiving the BSMs, each PIM device compares the C-BSR addresses and priorities to elect the BSR.
  - RP election process: The C-RPs periodically send advertisement packets to the BSR in unicast mode to advertise the C-RP addresses, priorities, and addresses of the served groups. The BSR collects the information as RP-Set, encapsulates the information in a BSM, and sends the messages to each PIM device in the network. Upon receiving the RP-Set, the PIM devices in the network use the same algorithms for computation to obtain the RP that serves each group. Each PIM device obtains the RP position of each group. Figure 1-2 shows the schematic diagram of dynamic RP election.

Figure 1-2 Schematic Diagram of Dynamic RP Election



6. Multicast Source Registration

Figure 1-3 Schematic Diagram of Multicast Source Registration



As shown in Figure 1-3, when a multicast source sends data to a group, the source DR sends a register message to the RP so that the RP obtains the source information and a multicast packet and forwards the multicast packet to the members in the group. The forwarding process is described as follows:

(1) The multicast source sends a multicast packet to the source DR.

(2) The source DR encapsulates the multicast packet in a register message and sends the message to the RP in unicast mode.

(3) Upon receiving the register message, the RP decapsulates the message and forwards the multicast packet to the members in a group via the RPT. Meanwhile, the RP sends an (S, G) join packet to the source. The PIM devices on the route create (S, G) entries, and finally create an SPT from the source to the RP.

(4) The source DR S forwards multicast packets based on this SPT. The multicast data is sent to the RP in the form of multicast packets.

(5) Upon receiving multicast packets from the source, the RP discards the register message and sends a register-stop message to the source.

(6) Upon receiving the register-stop message, the source DR stops encapsulating the register message, forwards multicast packets via the SPT, and periodically sends a register-probe message to the RP.

(7) Upon receiving the register-probe message, the RP sends a register-stop message to the source DR and updates the (S, G) entries.

(8) Upon receiving the register-stop message, the source DR continues forwarding multicast packets via the SPT without encapsulating the register message.

7. RPT Construction

When a group member joins the network, the DR connecting to the group member sends a join packet to the RP. If a multicast source has sent a multicast packet to the RP, the multicast packet will be sent to the group member via the RPT.

The RPT construction procedure is as follows:

- When a member DR receives an MLD (*, G) INCLUDE Report packet, if the member DR is not an RP of the group G, the member DR sends a (*, G) join packet to the RP and the multicast devices on the route create the (*, G) entries hop by hop to generate an RPT that uses the RP as the root.
- During RPT construction, each PIM device checks the reverse path forwarding (RPF) when sending a join packet to the RP to find the unicast route to the RP. The outbound interface of the unicast route is an uplink interface, and the next hop of the unicast route is the RPF neighbor. The join packet is sent from the member DR to the RP.

8. SPT Switchover

In the PIM-SMv6 network of the ASM model, one or multiple multicast groups correspond to one RP. Before SPT switchover, all packets of multicast groups sent to the RP service must be transitioned by the RP. When the sending rate of multicast packets grows, the RP load is increased. To solve this problem, the PIM-SMv6 relieves the RP load by SPT switchover. SPT switchover can be triggered by the RP or a member DR.

- SPT switchover triggered by the RP

  After receiving a register message from the source DR, the RP decapsulates the register message, forwards the multicast packets in the message to the group members via the RPT, and sends an (S, G) join packet to the source DR. The PIM multicast devices on the route create (S, G) entries hop by hop to create an SPT from the RP to the source.
- SPT switchover triggered by a member DR

  a When receiving the first multicast packet from the RP, the member DR obtains the source address.

  b The member DR sends an (S, G) join packet to the source. The PIM devices on the route create (S, G) entries and create an SPT from the member DR to the source DR.

  c After the SPT is created, the member DR sends a prune packet to the RP hop by hop and removes the downlink interface from the (*, G) entries. After the pruning, the RP does not forward multicast packets to the member DR via the RPT.

  d The SPT from the member DR to the source DR does not pass the RP. The RP sends a prune packet to the source DR to remove the downlink interface from the (S, G) entries. After the pruning, the source DR does not forward packets to the RP via the original "RP-source DR" SPT.

1.2.2 SSM Model

1. Basic Principles

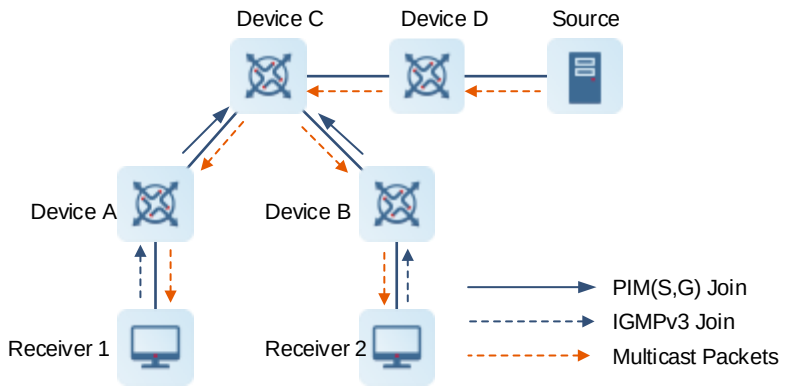
In the SSM model, members in a multicast group can specify to receive or reject data from a multicast source. The group members get to know the (S, G) entries of sources through access to the server or receiving advertisements. After understanding requirement of group members, the member DR sends a join packet to the source DR. This join packet is transmitted to the multicast source hop by hop to create an SPT from the source to the group members.

Note

- To implement the SSM model on IPv6, complete multicast interconnection through the PIM-SMv6 and configure MLDv2 to manage relationship between the hosts and devices.
- SSM model requirements: The hosts must know the addresses of multicast sources in advance using other network services so that the hosts can select multicast sources.

- On the devices that reside on the route from the hosts to the multicast source, the PIM-SMv6 and SSM functions must be enabled.

Figure 1-4 SSM Model



Caution

After the SSM function is enabled, the default group range of the SSM is FF3x::/32 (x cannot be 1 or 2). You can modify the group range of the SSM using commands.

In the SSM model, the key mechanisms of PIM-SMv6 include neighbor creation, DR election, and SPT creation.

2. PIMv6 Neighbor Creation

For more information about the PIMv6 neighbor creation mechanism in the SSM model, see the PIMv6 neighbor creation mechanism in the ASM model in 1.2.1 2. PIMv6 Neighbor Creation.

3. DR Election

For more information about the DR election mechanism in the SSM model, see the DR election mechanism in the ASM model in 1.2.1 3. DR Election.

4. SPT Construction

The SPT construction mechanism is as follows:

(1) The member DR learns through MLDv2 that a group member wants to receive data of a multicast source and sends an (S, G) join packet to the source hop by hop.

(2) The PIMv6 multicast devices on the route receive the (S, G) join packet and create the (S, G) entries, creating an SPT from the group member to the source.

(3) After the SPT is created, the multicast source distributes the multicast packets to the group member via the SPT.

1.2.3 Protocols and Standards

- RFC4601: Protocol Independent Multicast-Sparse Mode (PIM-SM)
- RFC5059: Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)

- RFC3962: Protocol Independent Multicast-Dense Mode protocol
- RFC4607: Source-Specific Multicast for IP

1.3 Restrictions and Guidelines

- Before PIM-SMv6 is enabled, enable the multicast routing and forwarding function in global configuration mode. Otherwise, multicast packets cannot be sent even if PIM-SMv6 is enabled.
- In the IPv6 multicast network, the PIM (IPv6) protocol must be run on all L3 devices. Otherwise, a forwarding route cannot be created.

1.4 Configuration Task Summary

The PIM-SMv6 configuration includes the following tasks:

(1) Enabling the PIM-SMv6 Function

(2) Configuring a model for PIM-SMv6. Select one of the following to configure:

- Configuring PIM-SMv6 in the ASM Model
- Configuring PIM-SMv6 in the SSM Model

(3) Configuring PIM-SMv6 Neighbor Parameters. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Neighbor Message Time Parameters
- Configuring Neighbor Tracking
- Configuring Neighbor Filtering

(4) (Optional) Configuring DR Priority

(5) Configuring Parameters of the Join/Prune Packets. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring Join/Prune Packet Sending Interval
- Configuring the Prune Delay

(6) (Optional) Enabling PIM-SMv6 BFD Correlation

1.5 Enabling the PIM-SMv6 Function

1.5.1 Overview

Neighbor relationship must be created between PIM multicast devices to form a PIM-SMv6 network, so that PIM control messages and multicast packets can be transmitted on the network. The PIM-SMv6 function must be configured on all interfaces so that PIM neighbor creation, multicast entry creation, and multicast packet forwarding can be successful.

In a PIMv6 network, if you want an interface, for example, a stub network device interface connecting to hosts, to receive multicast packets without involving the PIMv6 network topology construction, you can set the interface to the PIM-SMv6 passive mode. After the PIM-SMv6 passive mode is configured, the interface does not process PIM packets. This improves device performance.

1.5.2 Restrictions and Guidelines

- The IPv6 multicast routing function must be enabled on each multicast device.
- The PIM-SMv6 function should be enabled on the following interfaces: interfaces interconnecting multicast devices, interfaces connecting the static RP, C-RP and C-BSRs, and interfaces connecting multicast sources or hosts.
- PIMv6 interfaces must be L3 interfaces, including: routing, L3AP, switch virtual interface (SVI), and loopback interfaces.

1.5.3 Prerequisites

All PIM interfaces can be reached via IPv6 unicast routes.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IPv6 multicast routing.

ipv6 multicast-routing

The IPv6 multicast routing function is disabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Enable the PIM-SMv6 function.

ipv6 pim sparse-mode

The PIM-SMv6 function is disabled by default.

(6) (Optional) Enable the PIM-SMv6 passive mode.

ipv6 pim sparse-mode passive

The PIM-SMv6 passive mode is disabled by default.

1.6 Configuring PIM-SMv6 in the ASM Model

1.6.1 Overview

The PIM-SMv6 network supports the multicast service in the ASM and SSM models. Either one model or two models can be configured.

PIM-SMv6 in the ASM model can provide hosts with multicast services of any source. A host joining a multicast group can receive multicast packets destined to this multicast group from any source.

If you require a PIMv6 network to support the multicast service in the ASM model, an RP must be configured. There are three methods to configure an RP:

- Configure a static RP.
- Configure a dynamic RP.

- Configure static and dynamic RPs. If static and dynamic RPs are available at the same time, dynamic RPs prevail.

1.6.2 Configuration Tasks

The PIM-SMv6 configuration in the ASM model includes the following tasks. Configure at least one RP, either dynamic or static. You can also configure both a static RP and a dynamic RP.

- Configuring a Static RP
- Configuring a Dynamic RP
  - Configuring C-BSRs and Related Parameters
  - Configuring C-RPs and Related Parameters
  - (Optional) Configuring Registration Parameters
- (Optional) Configuring the Last Hop Device to Switch over from the RPT to SPT

1.6.3 Prerequisites

In the PIM-SMv6 multicast network, all nodes are reachable via IPv6 unicast routes.

1.6.4 Configuring a Static RP

1. Overview

You can manually configure a static RP to prevent frequent packet interaction between the BSR and C-RPs or between the BSR and PIM multicast devices and avoid bandwidth occupation. If the multicast network is simple and small, you can configure a static RP.

2. Restrictions and Guidelines

- Static RPs must be configured on every multicast device.
- The multicast device selected as a static RP must boast high performance.
- You are advised to use the loopback interface as a static RP address.
- Static RPs configured on multicast devices should be consistent, including RP address and address range of the served groups.
- If multiple static RPs are configured to correspond to different addresses of groups, the RPs can implement load balancing.
- If multiple static RPs serve the same group, the static RP with a larger IPv6 address is selected first.
- You can use the control list to configure an RP to serve multiple (referencing an ACL) or all (not referencing an ACL) multicast groups. However, an RP can adopt only one configuration.

3. Prerequisites

Before an address range of a group is configured for an RP, ensure that the corresponding ACL is created and specify a multicast group range for the static RP to serve. For more information about ACL configuration, see *Configuring ACL*.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static RP.

ipv6 pim rp-address *ipv6-rp-address* [*acl-name*]

No static RP is configured by default.

1.6.5 Configuring C-BSRs and Related Parameters

1. Overview

In the PIM-SMv6 domain of the ASM model, a unique BSR must be available. The BSR collects and releases RP information.

- The BSR is elected from C-BSRs based on rules. The election rules are as follows:
  - a The priorities of the C-BSRs are compared. The device with a higher priority is selected.
  - b If the priorities are the same, the IP addresses are compared. The device with a larger IP address is selected.

  The winner is elected as the BSR in the domain and periodically sends BSMs in the domain. A BSM contains the BSR IP address, RP-Set and hash mask information. The hash mask is used for hash calculation during C-RP election. In the hold time of a BSM, if other C-BSRs do not receive the BSM from the BSR, the BSR is considered unreachable and a new round of BSR election is initiated.
- To avoid fraud by an illegitimate BSR, a BSR range can be specified on all PIM devices in the domain so that the PIM devices ignore a BSM that is sent from an illegitimate BSR.
- To limit BSM flooding, you can configure a BSR border on an interface. Upon receiving BSMs, this interface discards the BSMs without forwarding them. This limits the BSM flooding.

2. Restrictions and Guidelines

- C-BSRs must be configured on one or multiple multicast devices.
- The multicast devices selected as C-BSRs must boast high performance. The C-RPs and C-BSRs can reside on the same or different multicast devices.
- You are advised to use the loopback interface as a C-BSR address.
- If multiple C-BSRs are configured, they can implement redundancy backup.
- You are advised to configure a valid BSR address range on all PIM devices in the domain.
- A BSR border must be configured on the interface between domains.

3. Prerequisites

- Enabling the PIM-SMv6 Function.
- Before a valid BSR address range is configured on PIM devices, ensure that the corresponding ACL is created and specify a valid BSR range. For more information about ACL configuration, see *Configuring ACL*.

4. Procedure

(1) Configure C-BSRs and related parameters.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Configure C-BSRs.

ipv6 pim bsr-candidate *interface-type interface-number* [*hash-mask-length* [*priority-value*]]

No C-BSR is configured by default.

(2) (Optional) Configure a valid BSR address range on all PIM devices.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Configure a valid BSM address range on the PIM multicast devices.

ipv6 pim accept-bsr list *acl-name*

All BSMs are received by default.

(3) (Optional) Configure a BSR border on the interface between PIM-SMv6 domains.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Enter the interface configuration mode.

interface *interface-type interface-number*

d Configure a BSR border.

Ipv6 pim bsr-border

No BSR border is configured by default.

If multiple domains exist, the BSR border must be configured on the interface between two domains.

1.6.6 Configuring C-RPs and Related Parameters

1. Overview

- After a multicast device is configured as a C-RP, the C-RP periodically sends an advertisement packet to the BSR in unicast mode. The packet includes the RP priority, advertisement packet hold time (greater than the interval of sending the advertisement packet), RP address, address of the served group, and prefix of the multicast address. Upon receiving the advertisement packet, the BSR collects the information in the packet as RP-Set in the advertisement packet hold time, encapsulates the information in a BSM, and sends the message to all PIM devices. Upon receiving the BSM from the BSR, the PIM devices in the domain apply the same algorithms for hash calculation to calculate the C-RP serving each multicast group. After the advertisement packet hold time expires, if the BSR does not receive a next advertisement packet from the C-RP, this C-RP is considered unreachable.
- To prevent fraud by an illegitimate C-RP, a C-RP range can be specified on the BSR. If an advertisement packet comes from an illegitimate C-RP, the packet is ignored.
- The BSR can determine whether to receive an advertisement packet with the prefix of the multicast address

being 0 from a C-RP. When the prefix of the multicast address is 0, this C-RP serves all multicast groups.

- When receiving the BSM from the BSR, each PIM multicast device in the domain applies rules to select the RP. The RP election rules are as follows:
  - a The address of the multicast group that a host joins is compared with the mask length of the group address range that the C-RP serves. The device with the longest mask is selected.
  - b If the addresses are consistent with the mask length, the priorities of the C-RPs are compared. The device with the smallest priority value is selected.
  - c If the priorities are consistent, hash values are calculated and compared. The device with the largest hash value is selected.
  - d If the hash values are the same, the IP addresses of the C-RPs are compared. The device with the largest IP address is selected.

2. Restrictions and Guidelines

- C-RPs must be configured on one or multiple multicast devices.
- The multicast devices selected as C-RPs must boast high performance. The C-RPs and C-BSRs can reside on the same or different multicast devices.
- You are advised to use the loopback interface as a C-RP address.
- If multiple C-RPs are configured to serve the same group, they can implement redundancy backup.
- If multiple C-RPs are configured to serve different groups, they can implement load balancing.
- A valid C-RP range can be configured on the BSR.
- To specify a group range for C-RPs to serve, you can add the ACL option to the **ip pim rp-candidate** command. The group range is calculated based on the permit access control entry (ACE), rather than the deny ACE.

3. Prerequisites

- Enabling the PIM-SMv6 Function.
- If the **group-list** parameter is used to limit the range of groups served by the RP, ensure that the corresponding ACL is created and specify a multicast group range for the RP to serve. For more information about ACL configuration, see *Configuring ACL*
- Before a valid C-RP address range is configured on PIM BSRs, ensure that the corresponding ACL is created and specify a multicast group range for the static RP to serve. For more information about ACL configuration, see *Configuring ACL*.

4. Procedure

- Configure a C-RP and related parameters.
  - a Enter the privileged EXEC mode.

    enable
  - b Enter the global configuration mode.

    configure terminal
  - c Configure a C-RP.

ipv6 pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *acl-name*]

No C-RP is configured by default.

- (Optional) Configure the BSR to receive C-RP advertisement packets with the prefix of the multicast address being 0. This C-RP serves all the multicast groups.

  a Enter the privileged EXEC mode.

  enable

  d Enter the global configuration mode.

  configure terminal

  e Configure the BSR to receive advertisement packets from the C-RP that serves all multicast groups.

  ipv6 pim accept-crp-with-null-group

  The function for the BSR to receive advertisement packets from the C-RP that serves all multicast groups is disabled by default.

  You are advised to enable this function on all C-BSRs.

- (Optional) Configure a valid C-RP range on the BSR.

  a Enter the privileged EXEC mode.

  enable

  f Enter the global configuration mode.

  configure terminal

  g Configure a valid C-RP range.

  ipv6 pim accept-crp list *acl-name*

  The C-BSRs receive all external C-RP advertisement packets by default.

  You are advised to enable this function on all C-BSRs.

- (Optional) Configure all PIM multicast devices to ignore RP priority and reselect an RP.

  a Enter the privileged EXEC mode.

  enable

  h Enter the global configuration mode.

  configure terminal

  i Configure all PIM multicast devices to ignore the RP priority for RP election.

  ipv6 pim ignore-rp-set-priority

  If the address of the multicast group that a host joins is consistent with the mask length of the group address range that the C-RPs serve, the RP with the highest priority is selected by default.

  You can configure each multicast device to ignore C-RP priority.

- (Optional) Configure static RP priority to be higher than dynamic RP priority on all PIM multicast devices.

  a Enter the privileged EXEC mode.

  enable

  j Enter the global configuration mode.

configure terminal

k Configure the static RP priority.

ipv6 pim static-rp-preferred

The dynamic RP priority is higher than the static RP priority by default.

You can configure each multicast device to ignore dynamic RP priority.

1.6.7 Configuring Registration Parameters

1. Overview

When a multicast source sends multicast data, the data arrives at the source DR first. Upon receiving the multicast data, the source DR encapsulates the multicast data as a register message and sends the message to the RP. Related parameters of the register message are configured on the source DR and RP.

- You can configure the following parameters on the source DR:
  - RP reachability checking: Before sending a register message, the source DR determines whether the RP is reachable. If the RP is reachable, the message is sent. Otherwise, the message is not sent.
  - Limit on the rate of sending the register message: The rate of sending each register message in (S, G) status is limited. If multiple register messages in (S, G) status are sent from the same source, the rate of the register messages is limited to the product of *N* × Limit value.
  - Source address in the register message: The source address in the register message is the address of the DR interface connected to the multicast source by default. If a security policy is configured on the RP to filter out this address, the RP does not receive register messages from this source DR. In this case, you can specify a reachable source address as the source address of the register message.
  - Register suppression time: When the RP receives multicast packets sent by the multicast source via the SPT, the RP sends a register-stop message to the source DR. Within the register suppression time, the source DR stops encapsulating the register message and sends multicast packets to the RP via the SPT. After the register suppression time expires, if the source DR does not receive another register-stop message from the RP, the source DR continues to encapsulate the register message and send the message to the RP.
  - Null message detection time: Before the register suppression time expires, the RP receives a null message from the source DR, refreshes the local (S, G) entries, and sends a register-stop message to the source DR so that the source DR refreshes the register suppression timer. Otherwise, the source DR continues to encapsulate the register message and send multicast packets to the RP in the form of the register message.
- You can configure the following parameters on the RP:
  - (S, G) address range of source: Provide multicast services for hosts in the permitted multicast group in the ASM model. After this parameter is configured, the RP replies a register-stop message upon receiving data from an unauthorized source.
  - Length of register message checksum: Adjust the calculation method of the register message checksum and calculate the checksum of the entire PIM protocol packets (including encapsulated multicast packets) or the checksum of PIM headers of separate register messages.
  - Register message decapsulation and delivery to downlink interface: Configure this parameter on the RP to decapsulate the received register message and forward the multicast packets in the register

message.

- Register message (S, G) entry timeout period: Configure this parameter to configure the timeout period of (S, G) entries. The (S, G) entries age if no packet is received within the register message timeout period.

2. Restrictions and Guidelines

- The source address in the specified register message must be reachable in unicast mode. You are advised to use the loopback interface of the source DR as the source address of the register message.
- If the **ip pim rp-register-kat** command is not configured, modifying the register suppression time on the RP changes the (S, G) entry timeout period.
- Configuring a limit to the register message rate reduces the load of the source DR and RP. Only register messages under the limit are sent.
- The register-probe time cannot be greater than a half of the register suppression time. Otherwise, the configuration failed and an alarm is generated.
- The sum of the three times of register suppression time and the register-probe time does not exceed 65,535. Otherwise, the configuration failed and an alarm is generated.

3. Prerequisites

- Enabling the PIM-SMv6 Function.
- Before an (S, G) address range is configured for the source, if the **list** parameter is specified, ensure that the corresponding ACL is created and specify an (S, G) address range for the source. For more information about ACL configuration, see *Configuring ACL*
- Before an (S, G) address range is configured for the source, if the **route-map** parameter is specified, ensure that the corresponding route map is created and specify an (S, G) address range for the source. For more information about route map configuration, see *Configuring Routing Policies*.
- Before the register message checksum calculation is applied to entire packets, if the **group-list** parameter is specified, ensure that the corresponding ACL is created and specify the register message checksum calculation to apply to the entire packets in a multicast group address range. For more information about ACL configuration, see *Configuring ACL*.

4. Procedure

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configure registration parameters on the source DR.

  a Enter the privileged EXEC mode.

  enable

  b Enter the global configuration mode.

  configure terminal

  c Enable RP reachability checking on the source DR.

  ipv6 pim register-rp-reachability

  The RP reachability checking function is disabled by default.

  d Limit the rate of sending register messages on the source DR.

ipv6 pim register-rate-limit *rate*

The sending rate of register messages is not limited by default.

e Configure a source address in the register messages on the source DR.

ipv6 pim register-source { *ipv6-local-address* | *interface-type interface-number* }

The source IP address in the register messages is the address of the DR interface connected to the source by default.

f Configure the register suppression time on the source DR.

ipv6 pim register-suppression *suppression-time*

The default register suppression time is **60** seconds.

g Configure the null message detection time on the source DR.

ipv6 pim probe-interval *interval*

The default register-probe time is **5** seconds.

- Configure registration parameters on the RP.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Configure the (S, G) address range for the source on the RP.

ipv6 pim accept-register { **list** *acl-name* | **route-map** *route-map-name* } *

The (S, G) address range of register messages is not limited by default. The RP receives register messages with any (S, G) address.

You can configure to filter the source register message information on all C-RP or static RP multicast devices.

d Enable register message checksum calculation to be applied to the entire packets on the RP.

ipv6 pim register-checksum-wholepkt [**group-list** *acl-name*]

By default, the register message checksum of headers of only PIM packets and register messages, rather than the entire packets, is calculated.

If the **group-list** parameter is not specified, this configuration applies to all group addresses.

e Configure the timeout period for the (S, G) entries created upon receiving the register message on the RP.

ipv6 pim rp-register-kat *interval*

By default, the timeout period for the (S, G) entries is the sum of three times of the register suppression time and the register-probe time.

You can configure the (S, G) entry timeout period on all C-RP or static RP multicast devices.

1.6.8 Configuring the Last Hop Device to Switch over from the RPT to SPT

1. Overview

If the multicast traffic in a network is heavy, the RP easily gets overloaded and then faulty. To relieve the RP load, you can initiate SPT switchover through the member DR. You can specify multicast groups to perform SPT switchover.

2. Prerequisites

- Enabling the PIM-SMv6 Function.
- Before an address range of a group is configured for SPT switchover, ensure that the corresponding ACL is created and specify a multicast group range for SPT switchover. For more information about ACL configuration, see *Configuring ACL*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the SPT switchover function.

ipv6 pim spt-threshold [**group-list** *acl-name*]

The SPT switchover function is disabled by default.

If the **group-list** parameter is not specified, all groups support SPT switchover.

1.7 Configuring PIM-SMv6 in the SSM Model

1.7.1 Overview

The PIM-SMv6 function in the SSM model can provide specified source services for hosts so that the hosts can determine to receive or reject multicast data of specified sources based on needs.

1.7.2 Restrictions and Guidelines

- If you require a PIM network to support the multicast service in the SSM model, the SSM function must be enabled.
- The SSM function must be enabled on each multicast device.
- The address range of SSM groups configured on all multicast devices must be consistent.
- MLDv2 or SSM mapping must be enabled.

1.7.3 Prerequisites

- In the multicast network, all nodes are reachable via IPv6 unicast routes.
- Enabling the PIM-SMv6 Function.
- Before an SSM group range is configured using an ACL, ensure that the corresponding ACL is created and specify an SSM multicast group range. For more information about ACL configuration, see *Configuring ACL*.

1.7.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the SSM function.

ipv6 pim ssm { **default** | **range** *acl-name* }

The SSM function is disabled by default.

1.8 Configuring PIM-SMv6 Neighbor Parameters

1.8.1 Overview

PIM multicast devices transmit Hello messages to discover neighbors, coordinate protocol parameters and maintain neighbor relationships.

1.8.2 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Neighbor Message Time Parameters
- Configuring Neighbor Tracking
- Configuring Neighbor Filtering

1.8.3 Prerequisites

- In the multicast network, all nodes are reachable via IPv6 unicast routes.
- Enabling the PIM-SMv6 Function.

1.8.4 Configuring the Neighbor Message Time Parameters

1. Overview

The neighbor message time parameters include hello message sending interval and hello message sending delay.

- The hello message sending interval can be configured, and the hello message hold time is 3.5 times the hello message sending interval. If no new hello message is received within the hello message hold time, the neighbor is considered unreachable.
- When the PIM interface is enabled or detects a new neighbor, random time is generated and it is referred to as hello message sending delay. Within the delay time, the interface sends hello messages out.

2. Restrictions and Guidelines

If the hello message hold time is greater than 65,535 seconds, the hello message sending interval is automatically set to 18,725 seconds.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the neighbor message time parameters. Configure at least one of the tasks.

- Configure the hello message sending interval.

  ipv6 pim query-interval *interval*

  The hello message is sent at an interval of **30** seconds by default.

- Configure the hello message sending delay.

  ipv6 pim triggered-hello-delay *delay*

  The default hello message sending delay is **5** seconds.

1.8.5 Configuring Neighbor Tracking

1. Overview

After the suppression capability of an interface is enabled, when a multicast device plans to send a join packet to an uplink multicast device but it receives a join packet sent from the neighbor to the uplink multicast device, this local multicast device suppresses its own join packet. If the suppression capability of the interface is disabled, the join packet can be sent. When the suppression capability of downlink hosts is disabled, an uplink device can determine the number of the downlink hosts based on the quantity of received join packets. This is neighbor tracking.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the neighbor tracking function.

ipv6 pim neighbor-tracking

The neighbor tracking function is disabled by default.

1.8.6 Configuring Neighbor Filtering

1. Overview

The neighbor filtering function can protect neighborhood. Controlling neighbors can strengthen PIM network security and limit the valid address range of neighbors. If a neighbor is filtered out based on an access filtering list, PIM-SMv6 does not create peer relationship with the neighbor or stops the peer relationship with this neighbor.

2. Prerequisites

Before an access filtering list is configured, ensure that the corresponding ACL is created and specify a valid neighbor address range. For more information about ACL configuration, see *Configuring ACL*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the neighbor filtering function.

ip pim neighbor-filter *acl-name*

The neighbor filtering function is disabled by default.

1.9 Configuring DR Priority

1.9.1 Overview

In a network segment shared by multicast sources and group members, multiple PIM multicast devices exist. The PIM multicast devices elect a DR based on neighbor messages. A device with the highest priority is selected. If the priorities are the same or some PIM devices do not support the DR priority function, the IP addresses are compared and the PIM multicast device with the largest IP address is selected. The selected PIM device functions as a DR, transmits protocol packets between the sources and members, and forwards multicast packets.

1.9.2 Prerequisites

- In the multicast network, all nodes are reachable via IPv6 unicast routes.
- Enabling the PIM-SMv6 Function.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a DR priority in hello messages.

ipv6 pim dr-priority *priority-value*

The default DR priority in hello messages is **1**.

1.10 Configuring Parameters of the Join/Prune Packets

1.10.1 Overview

A device sends a join packet to request an uplink device to forward multicast packets and sends a prune packet to request the uplink device to stop forwarding multicast packets. The request route is referred to as an RPT or SPT.

1.10.2 Restrictions and Guidelines

- The network administrator must ensure that the prune override interval is smaller than the join-prune packet hold time. Otherwise, a short interrupt may occur.
- When the PIM multicast device receives a prune message from an uplink interface, there are other downlink devices existent in the shared network segment. If this PIM multicast device still needs to receive multicast data, the PIM multicast device must send a prune override message to the uplink device within the override interval.

1.10.3 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring Join/Prune Packet Sending Interval
- Configuring the Prune Delay

1.10.4 Prerequisites

Enabling the PIM-SMv6 Function.

1.10.5 Configuring Join/Prune Packet Sending Interval

1. Overview

A PIM device periodically sends the join/prune packet to an uplink device to update the forwarding status. The join packet is used to request data forwarding and the prune packet is used to stop data forwarding. Upon receiving the join/prune packet, the uplink device starts the join/prune packet hold time timer.

- If a join packet hold time timer expires, the PIM device is suppressed to forward multicast packets of the corresponding multicast group through the downlink interface.
- If a prune packet hold time timer expires, the PIM device is restored to forward the multicast packets of the corresponding multicast group through the downlink interface.

2. Restrictions and Guidelines

The join/prune packet sending interval must be smaller than the join/prune packet hold time. Generally, the join/prune packet hold time is 3.5 times the join/prune packet sending interval.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the join/prune packet sending interval.

ipv6 pim jp-timer *interval*

The join/prune packet is sent at an interval of **60** seconds by default.

1.10.6 Configuring the Prune Delay

1. Overview

Upon receiving a prune packet from a downlink device, the multicast device does not perform prune immediately and it waits for a period of time. This period of time is divided into two parts: The part from the time when the multicast device receives a prune message to the time when the multicast device sends the prune message to the uplink device is referred to as the propagation delay; the part from the time when the PIM device receives a prune packet to the time when the device continues to forward the multicast packets to a downlink device is referred to as the override interval. The period from the time when the multicast device receives a prune message to the time when the prune action is performed is the sum of the propagation delay and the override interval.

2. Restrictions and Guidelines

In the period from the time when the multicast device receives a prune message to the time when the prune action is performed, if the PIM device receives a prune override message from the downlink interface, the PIM device cancels pruning.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the prune message propagation delay.

ipv6 pim propagation-delay *propagation-delay*

The default propagation delay of an interface is **500** ms.

(5) Configure the prune override interval.

ipv6 pim override-interval *override-interval*

The default prune override interval is **2500** ms.

1.11 Enabling PIM-SMv6 BFD Correlation

1. Overview

In some shared multicast network, PIM neighbor status change triggers re-initiation of some mechanisms, for example, DR election mechanism. Generally, a PIM neighbor triggers a new round of election after the neighborhood times out, causing multicast data interruption. PIM bidirectional forwarding detection (BFD) correlation can quickly detect link status and neighbor faults in a shared network segment and trigger a new

round of DR election. This reduces multicast data transmission interrupt time and ensures reliability of the multicast network.

2. Restrictions and Guidelines

- If DR or assertion election is required in a multicast network, you are advised to enable PIM-SMv6 BFD correlation.
- The PIM BFD function must be enabled on the interconnection interface of the multicast devices.
- PIM interfaces must be L3 interfaces, including: routing, L3AP, switch virtual interface (SVI), and loopback interfaces.

3. Prerequisites

- In the network, all nodes are reachable via IPv6 unicast routes.
- Enabling the PIM-SMv6 Function.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable PIM-SMv6 BFD correlation.

ipv6 pim bfd

PIM-SMv6 BFD correlation is disabled by default.

1.12 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear ipv6 pim sparse-mode bsr rp-set *	Clears dynamic RP information.
clear ipv6 pim sparse-mode track	Resets the statistic start time and clears the counter of the PIMv6 packets.
show ipv6 pim sparse-mode bsr-router	Displays details about the BSR.

Command	Purpose
show ipv6 pim sparse-mode interface [*interface-type interface-number*] [**detail**]	Displays PIM-SMv6 information of an interface.
show ipv6 pim sparse-mode local-members [*interface-type interface-number*]	Displays local MLD information of a PIM-SMv6 interface.
show ipv6 pim sparse-mode mroute [*ipv6-group-or-source-address* [*ipv6-group-or-source-address*]]	Displays PIM-SMv6 routing information.
show ipv6 pim sparse-mode neighbor [**detail**]	Displays PIM-SMv6 neighbor information.
show ipv6 pim sparse-mode nexthop	Displays next hop information, including interface number, address, and metric value of a next hop.
show ipv6 pim sparse-mode rp mapping	Displays all RPs and the groups served by the RPs on the local device.
show ipv6 pim sparse-mode rp-hash *ipv6-group-address*	Displays RP information corresponding to a group address.
show ipv6 pim sparse-mode track	Displays the number of PIM packets sent and received since the statistic start time.

1.13 Configuration Examples

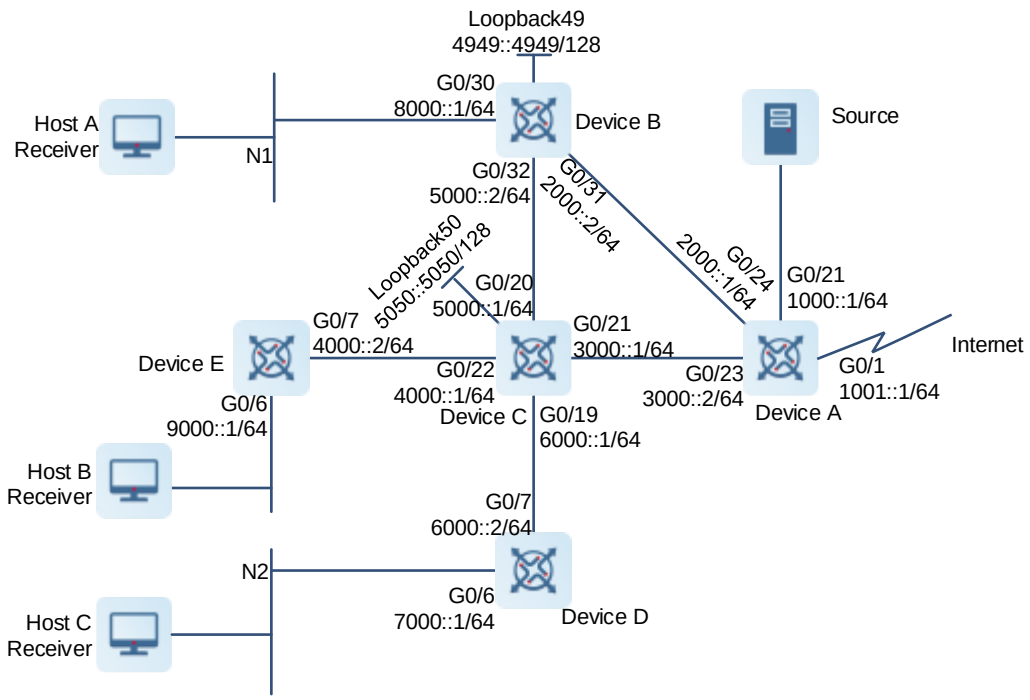
1.13.1 Configuring Basic Functions of PIM-SMv6 in the ASM Model

1. Requirements

As shown in Figure 1-5, the internal network is connected to the Internet. The PIM-SMv6 protocol is configured on each multicast device to provide ASM multicast services for hosts in networks N1 and N2 so that hosts joining a multicast group can receive multicast data destined to this multicast group from any multicast source, including video-on-demand information.

2. Topology

Figure 1-5 PIM-SMv6 Multicast Network Topology in the ASM Model



3. Notes

- Configure IPv6 addresses and unicast routing protocols for multicast devices. The PIMv6 protocol in a multicast domain depends on unicast routing protocols. Normal communication of unicast routing lays a foundation of multicast routing. Ensure that each PIM node is reachable via unicast routes.
- Enable the IPv6 multicast function on all multicast devices. Enabling the multicast function is a prerequisite of PIM-SMv6 configuration.
- Enable the basic functions of PIM-SMv6 on all interfaces of the multicast devices. The other functions of PIM-SMv6 can be enabled only after the basic functions of PIM-SMv6 are enabled.
- Enable the MLD function on the interface connected to hosts so that the hosts can join or leave a multicast group by sending MLD messages. The multicast devices acting as leaf nodes maintain group membership based on the MLD protocol.
- Configure RPs. In the PIM-SMv6 network in the ASM model, the RP is a transitional station for forwarding multicast data. It is recommended that the multicast device with many traffic flows be configured as an RP, for example, device C in Figure 1-5.
- Configure a BSR border on the interface connected to the Internet. BSMs must be transmitted in the PIM-SMv6 domain within the border to improve the multicast controllability.

4. Procedure

(1) Configure IP addresses and enable unicast routing protocols on interfaces of different devices.

Configure an IPv6 address for the interface of Device A and configure the OSPFv3 protocol to implement internetworking.

```
DeviceA> enable
DeviceA# config terminal
DeviceA(config)# ipv6 router ospf 4949
DeviceA(config-router)# exit
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no switchport
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 address 1001::1/64
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# no switchport
DeviceA(config-if-GigabitEthernet 0/21)# ipv6 address 1000::1/64
DeviceA(config-if-GigabitEthernet 0/21)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/21)# exit
DeviceA(config)#interface gigabitEthernet 0/23
DeviceA(config-if-GigabitEthernet 0/23)# no switchport
DeviceA(config-if-GigabitEthernet 0/23)# ipv6 address 3000::2/64
DeviceA(config-if-GigabitEthernet 0/23)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/23)# exit
DeviceA(config)# interface gigabitEthernet 0/24
DeviceA(config-if-GigabitEthernet 0/24)# no switchport
DeviceA(config-if-GigabitEthernet 0/24)# ipv6 address 2000::1/64
DeviceA(config-if-GigabitEthernet 0/24)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/24)# exit
```

Configure IPv6 addresses on interfaces of device B, and configure the OSPFv3 protocol to implement internetworking.

```
DeviceB> enable
DeviceB# config terminal
DeviceB(config)# ipv6 router ospf 4949
DeviceB(config-router)# exit
DeviceB(config)# interface GigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# no switchport
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 address 8000::1/64
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 ospf 4949 area 0
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface GigabitEthernet 0/31
DeviceB(config-if-GigabitEthernet 0/31)# no switchport
DeviceB(config-if-GigabitEthernet 0/31)# ipv6 address 2000::2/64
DeviceB(config-if-GigabitEthernet 0/31)# ipv6 ospf 4949 area 0
DeviceB(config-if-GigabitEthernet 0/31)# exit
DeviceB(config)# interface GigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# no switchport
DeviceB(config-if-GigabitEthernet 0/32)# ipv6 address 5000::2/64
DeviceB(config-if-GigabitEthernet 0/32)# ipv6 ospf 4949 area 0
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface loopback 49
```

```
DeviceB(config-if-Loopback 49)# ipv6 address 4949::4949/128
DeviceB(config-if-Loopback 49)# ipv6 ospf 4949 area 0
DeviceB(config-if-Loopback 49)# exit
```

Configure IPv6 addresses on interfaces of device C, and configure the OSPFv3 protocol to implement internetworking.

```
DeviceC> enable
DeviceC# config terminal
DeviceC(config)# ipv6 router ospf 4949
DeviceC(config-router)# exit
DeviceC(config)# interface GigabitEthernet 0/19
DeviceC(config-if-GigabitEthernet 0/19)# no switchport
DeviceC(config-if-GigabitEthernet 0/19)# ipv6  address 6000::1/64
DeviceC(config-if-GigabitEthernet 0/19)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/19)# exit
DeviceC(config)#interface GigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# no switchport
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 address 5000::1/64
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# no switchport
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 address 3000::1/64
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface GigabitEthernet 0/22
DeviceC(config-if-GigabitEthernet 0/22)# no switchport
DeviceC(config-if-GigabitEthernet 0/22)# ipv6 address 4000::1/64
DeviceC(config-if-GigabitEthernet 0/22)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/22)# exit
DeviceC(config)# interface loopback 50
DeviceC(config-if-Loopback 50)# ipv6 address 5050::5050/128
DeviceC(config-if-Loopback 50)# ipv6 ospf 4949 area 0
DeviceC(config-if-Loopback 50)# exit
```

Configure IPv6 addresses on interfaces of device D, and configure the OSPFv3 protocol to implement internetworking.

```
DeviceD> enable
DeviceD# config terminal
DeviceD(config)# ipv6 router ospf 4949
DeviceD(config-router)# exit
DeviceD(config)# interface GigabitEthernet 0/6
DeviceD(config-if-GigabitEthernet 0/6)# no switchport
DeviceD(config-if-GigabitEthernet 0/6)# ipv6 address 7000::1/64
DeviceD(config-if-GigabitEthernet 0/6)# ipv6 ospf 4949 area 0
DeviceD(config-if-GigabitEthernet 0/6)# exit
DeviceD(config)# interface GigabitEthernet 0/7
```

```
DeviceD(config-if-GigabitEthernet 0/7)# no switchport
DeviceD(config-if-GigabitEthernet 0/7)# ipv6 address 6000::2/64
DeviceD(config-if-GigabitEthernet 0/7)# ipv6 ospf 4949 area 0
DeviceD(config-if-GigabitEthernet 0/7)# exit
```

Configure IPv6 addresses on interfaces of device E, and configure the OSPFv3 protocol to implement internetworking.

```
DeviceE> enable
DeviceE# config terminal
DeviceE(config)# ipv6 router ospf 4949
DeviceE(config-router)# exit
DeviceE(config)# interface GigabitEthernet 0/6
DeviceE(config-if-GigabitEthernet 0/6)# no switchport
DeviceE(config-if-GigabitEthernet 0/6)# ipv6 address 9000::1/64
DeviceE(config-if-GigabitEthernet 0/6)# ipv6 ospf 4949 area 0
DeviceE(config-if-GigabitEthernet 0/6)# interface GigabitEthernet 0/7
DeviceE(config-if-GigabitEthernet 0/7)# no switchport
DeviceE(config-if-GigabitEthernet 0/7)# ipv6 address 4000::2/64
DeviceE(config-if-GigabitEthernet 0/7)# ipv6 ospf 4949 area 0
DeviceE(config-if-GigabitEthernet 0/7)# exit
```

(2) Enable the multicast and PIM-SMv6 functions on all multicast devices, and enable the MLD function on all multicast devices connected to hosts.

Enable the multicast and PIM-SMv6 functions on device A.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface gigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/21)# exit
DeviceA(config)# interface gigabitEthernet 0/23
DeviceA(config-if-GigabitEthernet 0/23)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/23)# exit
DeviceA(config)# interface gigabitEthernet 0/24
DeviceA(config-if-GigabitEthernet 0/24)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/24)# exit
```

Enable the IPv6 multicast, IPv6-SMv6, and MLD functions on device B.

```
DeviceB(config)# ipv6 multicast-routing
DeviceB(config)# interface gigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface gigabitEthernet 0/31
DeviceB(config-if-GigabitEthernet 0/31)# ipv6 pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/31)# exit
DeviceB(config)# interface gigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# ipv6 pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface loopback 49
```

```
DeviceB(config-if-Loopback 49)# ipv6 pim sparse-mode
DeviceB(config-if-Loopback 49)# exit
```

Enable the IPv6 multicast and PIM-SMv6 functions on device C.

```
DeviceC(config)# ipv6 multicast-routing
DeviceC(config)# interface gigabitEthernet 0/19
DeviceC(config-if-GigabitEthernet 0/19)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/19)# exit
DeviceC(config)# interface gigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface gigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface gigabitEthernet 0/22
DeviceC(config-if-GigabitEthernet 0/22)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/22)# exit
DeviceC(config)# interface loopback 50
DeviceC(config-if-Loopback 50)# ipv6 pim sparse-mode
DeviceC(config-if-Loopback 50)# exit
```

Enable the IPv6 multicast, IPv6-SMv6, and MLD functions on device D.

```
DeviceD(config)# ipv6 multicast-routing
DeviceD(config)# interface gigabitEthernet 0/6
DeviceD(config-if-GigabitEthernet 0/6)# ipv6 pim sparse-mode
DeviceD(config-if-GigabitEthernet 0/6)# exit
DeviceD(config)# interface gigabitEthernet 0/7
DeviceD(config-if-GigabitEthernet 0/7)# ipv6 pim sparse-mode
DeviceD(config-if-GigabitEthernet 0/7)# exit
```

Enable the IPv6 multicast, IPv6-SMv6, and MLD functions on device E.

```
DeviceE(config)# ipv6 multicast-routing
DeviceE(config)# interface gigabitEthernet 0/6
DeviceE(config-if-GigabitEthernet 0/6)# ipv6 pim sparse-mode
DeviceE(config-if-GigabitEthernet 0/6)# exit
DeviceE(config)# interface gigabitEthernet 0/7
DeviceE(config-if-GigabitEthernet 0/7)# ipv6 pim sparse-mode
DeviceE(config-if-GigabitEthernet 0/7)# exit
```

(3) Configure RPs.

Note

There are two methods to configure RPs: dynamic RPs and static RPs. You can configure either or both types of RPs. If static and dynamic RPs are available at the same time, the dynamic RPs are preferred by default.

Configure dynamic RPs. One or multiple multicast devices in the PIM-SMv6 domain must be configured as C-RPs and C-BSRs. In this example, device B and device C are configured as C-RP and C-BSR. The address range of the served groups of the RP, as well as the interfaces of the C-RP and C-BSR are

configured on device B and device C. The loopback interface is configured as the interface of the C-RP and C-BSR.

Configure C-RP and C-BSR and address range of the served groups of the RP on device B.

```
DeviceB(config)# ipv6 pim bsr-candidate loopback 49
DeviceB(config)# ipv6 access-list mcast-ipv6-list
DeviceB(config-ipv6-acl)# permit ipv6 any ff13::/64
DeviceB(config)# ipv6 pim rp-candidate loopback 49 group-list mcast-ipv6-list
```

Configure C-RP and C-BSR and address range of the served groups of the RP on device C.

```
DeviceC(config)# ipv6 pim bsr-candidate loopback 50
DeviceC(config)# ipv6 access-list mcast-ipv6-list
DeviceC(config-ipv6-acl)# permit ipv6 any ff14::/64
DeviceC(config-std-nacl)# exit
DeviceC(config)# ipv6 pim rp-candidate loopback 50 group-list mcast-ipv6-list
```

Configure static RPs. The addresses of static RPs must be specified on all multicast devices.

Configure a static RP on device A.

```
DeviceA(config)# ipv6 pim rp-address 5050::5050
```

Configure a static RP on device B.

```
DeviceB(config)# ipv6 pim rp-address 5050::5050
```

Configure a static RP on device C.

```
DeviceC(config)# ipv6 pim rp-address 5050::5050
```

Configure a static RP on device D.

```
DeviceD(config)# ipv6 pim rp-address 5050::5050
```

Configure a static RP on device E.

```
DeviceE(config)# ipv6 pim rp-address 5050::5050
```

(4) Configure a BSR border on the device A interface connected to the Internet.

```
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 pim bsr-border
```

5. Verification

(1) Run the **show ipv6 pim sparse-mode interface** command to display the PIM-SMv6 running information on the interfaces.

The PIM-SMv6 running information on the interface of device A is as follows:

```
DeviceA> enable
DeviceA# show ipv6 pim sparse-mode interface
Interface                          VIFindex Ver/   Nbr    DR
                                          Mode   Count  Prior
GigabitEthernet 0/24                 3       v2/S   1      1
   Address      : fe80::2d0:f8ff:fe22:358d
   Global Address: 2000::1
   DR          : fe80::2d0:f8ff:feee:8c1f
GigabitEthernet 0/23                 2       v2/S   1      1
   Address      : fe80::2d0:f8ff:fe22:358d
```

```
   Global Address: 3000::2
   DR          : this system
GigabitEthernet 0/21                1       v2/S   0     1
   Address      : fe80::2d0:f8ff:fe22:358d
   Global Address: 1000::1
   DR          : this system
DeviceA#
```

The PIM-SMv6 running information on the interface of device B is as follows:

```
DeviceB> enable
DeviceB# show ipv6 pim sparse-mode interface
Interface                          VIFindex Ver/   Nbr    DR
                                          Mode   Count  Prior
GigabitEthernet 0/31                2       v2/S   1     1
   Address      : fe80::2d0:f8ff:feee:8c1f
   Global Address: 2000::2
   DR          : this system
GigabitEthernet 0/32                3       v2/S   1     1
   Address      : fe80::2d0:f8ff:feee:8c1f
   Global Address: 5000::2
   DR          : this system
GigabitEthernet 0/30                1       v2/S   0     1
   Address      : fe80::2d0:f8ff:feee:8c1f
   Global Address: 8000::1
   DR          : this system
Loopback 49                        4       v2/S   0     1
   Address      : fe80::2d0:f8ff:feee:8c1f
   Global Address: 4949::4949
   DR          : this system
DeviceB#
```

The PIM-SMv6 running information on the interface of device C is as follows:

```
DeviceC> enable
DeviceC# show ipv6 pim sparse-mode interface
Interface                          VIFindex Ver/   Nbr    DR
                                          Mode   Count  Prior
GigabitEthernet 0/21                3       v2/S   1     1
   Address      : fe80::274:9cff:feee:f49f
   Global Address: 3000::1
   DR          : fe80::2d0:f8ff:fe22:358d
GigabitEthernet 0/22                4       v2/S   1     1
   Address      : fe80::274:9cff:feee:f49f
   Global Address: 4000::1
   DR          : this system
GigabitEthernet 0/20                2       v2/S   1     1
   Address      : fe80::274:9cff:feee:f49f
   Global Address: 5000::1
```

```
   DR          : fe80::2d0:f8ff:feee:8c1f
GigabitEthernet 0/19                 1       v2/S   1     1
   Address      : fe80::274:9cff:feee:f49f
   Global Address: 6000::1
   DR          : this system
Loopback 50                          5       v2/S   0     1
   Address      : fe80::274:9cff:feee:f49f
   Global Address: 5050::5050
   DR          : this system
DeviceC#
```

The PIM-SMv6 running information on the interface of device D is as follows:

```
DeviceD> enable
DeviceD# show ipv6 pim sparse-mode interface
Interface                          VIFindex Ver/   Nbr    DR
                                          Mode   Count  Prior
GigabitEthernet 0/6                  1       v2/S   0     1
   Address      : fe80::274:9cff:fe11:c9e7
   Global Address: 7000::1
   DR          : this system
GigabitEthernet 0/7                  2       v2/S   1     1
   Address      : fe80::274:9cff:fe11:c9e7
   Global Address: 6000::2
   DR          : fe80::274:9cff:feee:f49f
DeviceD#
```

The PIM-SMv6 running information on the interface of device E is as follows:

```
DeviceE> enable
DeviceE# show ipv6 pim sparse-mode interface
Interface                          VIFindex Ver/   Nbr    DR
                                          Mode   Count  Prior
GigabitEthernet 0/6                  1       v2/S   0     1
   Address      : fe80::274:9cff:fec8:e27b
   Global Address: 9000::1
   DR          : this system
GigabitEthernet 0/7                  2       v2/S   1     1
   Address      : fe80::274:9cff:fec8:e27b
   Global Address: 4000::2
   DR          : fe80::274:9cff:feee:f49f
DeviceE#
```

(2) Run the **show ipv6 pim sparse-mode bsr-router** command to display the election information of the BSRs.

The BSR election information on device A is as follows:

```
DeviceA> enable
DeviceA# show ipv6 pim sparse-mode bsr-router
BSR address: 5050::5050
  Uptime:     00:05:28, BSR Priority: 64, Hash mask length: 126
```

```
  Expires:    00:01:54
  Role: Non-candidate BSR  Priority: 0, Hash mask length: 126
  State: Accept Preferred
DeviceA#
```

The BSR election information on device B is as follows:

```
DeviceB> enable
DeviceB# show ipv6 pim sparse-mode bsr-router
PIMv2 Bootstrap information
  BSR address: 5050::5050
  Uptime:     00:04:13, BSR Priority: 64, Hash mask length: 126
  Expires:    00:02:09
  Role: Candidate BSR  Priority: 64, Hash mask length: 126
  State: Candidate BSR

  Candidate RP: 4949::4949(Loopback 49)
    Advertisement interval 60 seconds
    Next Cand_RP_advertisement in 00:00:53
DeviceB#
```

The BSR election information on device C is as follows:

```
DeviceC> enable
DeviceC# show ipv6 pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 5050::5050
  Uptime:     00:04:25, BSR Priority: 64, Hash mask length: 126
  Next bootstrap message in 00:00:52
  Role: Candidate BSR  Priority: 64, Hash mask length: 126
  State: Elected BSR

  Candidate RP: 5050::5050(Loopback 50)
    Advertisement interval 60 seconds
    Next Cand_RP_advertisement in 00:00:44
```

The BSR election information on device D is as follows:

```
DeviceD> enable
DeviceD# show ipv6 pim sparse-mode bsr-router
PIMv2 Bootstrap information
  BSR address: 5050::5050
  Uptime:     00:06:00, BSR Priority: 64, Hash mask length: 126
  Expires:    00:01:21
  Role: Non-candidate BSR  Priority: 0, Hash mask length: 126
  State: Accept Preferred
DeviceD#
```

The BSR election information on device E is as follows:

```
DeviceE> enable
```

```
DeviceE# show ipv6 pim sparse-mode bsr-router
PIMv2 Bootstrap information
  BSR address: 5050::5050
  Uptime:     00:06:23, BSR Priority: 64, Hash mask length: 126
  Expires:    00:01:58
  Role: Non-candidate BSR  Priority: 0, Hash mask length: 126
  State: Accept Preferred
DeviceE#
```

(3) Run the **show ipv6 pim sparse-mode rp mapping** command to display the RP information on the multicast devices.

The RP information on device A is as follows:

```
DeviceA> enable
DeviceA# show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): ff13::/64
  RP: 4949::4949(Not self)
    Info source: 5050::5050, via bootstrap, priority 192
        Uptime: 03:10:58, expires: 00:01:32
Group(s): ff14::/64
  RP: 5050::5050(Not self)
    Info source: 5050::5050, via bootstrap, priority 192
        Uptime: 03:08:58, expires: 00:01:32
Group(s): ff00::/8, Static
    RP: 5050::5050(Not self), Static
        Uptime: 03:08:15
DeviceA#
```

The RP information on device B is as follows:

```
DeviceB> enable
DeviceB# show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): ff13::/64
  RP: 4949::4949(Self)
    Info source: 5050::5050, via bootstrap, priority 192
        Uptime: 03:12:31, expires: 00:02:08
Group(s): ff14::/64
  RP: 5050::5050(Not self)
    Info source: 5050::5050, via bootstrap, priority 192
        Uptime: 03:10:26, expires: 00:02:08
Group(s): ff00::/8, Static
    RP: 5050::5050(Not self), Static
        Uptime: 03:09:35
DeviceB#
```

The RP information on device C is as follows:

```
DeviceC> enable
```

```
DeviceC# show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): ff13::/64
  RP: 4949::4949(Not self)
    Info source: 4949::4949, via bootstrap, priority 192
        Uptime: 00:21:40, expires: 00:01:49
Group(s): ff14::/64
  RP: 5050::5050(Self)
    Info source: 4949::4949, via bootstrap, priority 192
        Uptime: 00:19:40, expires: 00:01:49
Group(s): ff00::/8, Static
    RP: 5050::5050(Self), Static
        Uptime: 00:18:52
DeviceC#
```

The RP information on device D is as follows:

```
DeviceD> enable
DeviceD# show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): ff13::/64
  RP: 4949::4949(Not self)
    Info source: 4949::4949, via bootstrap, priority 192
        Uptime: 00:21:59, expires: 00:01:31
Group(s): ff14::/64
  RP: 5050::5050(Not self)
    Info source: 4949::4949, via bootstrap, priority 192
        Uptime: 00:19:59, expires: 00:01:31
Group(s): ff00::/8, Static
    RP: 5050::5050(Not self), Static
        Uptime: 00:19:09
DeviceD#
```

The RP information on device E is as follows:

```
DeviceE> enable
DeviceE# show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): ff13::/64
  RP: 4949::4949(Not self)
    Info source: 4949::4949, via bootstrap, priority 192
        Uptime: 00:22:24, expires: 00:02:06
Group(s): ff14::/64
  RP: 5050::5050(Not self)
    Info source: 4949::4949, via bootstrap, priority 192
        Uptime: 00:20:24, expires: 00:02:06
Group(s): ff00::/8, Static
    RP: 5050::5050(Not self), Static
        Uptime: 00:19:31
```

```
DeviceE#
```

(4) Run the **show ipv6 pim sparse-mode mroute** command to display the multicast routing tables of PIM-SMv6. The multicast source (1001:: 2/64) sends traffic to the multicast groups (FF14::1/64) and (FF13::1/64). Host A joins the multicast group (FF14::1/64), and host B joins the multicast group (FF13::1/64).

The routing table information on device A is as follows:

```
DeviceA> enable
DeviceA# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 3
(S,G,rpt) Entries: 3
FCR Entries: 0
REG Entries: 3

(1000::2, ff13::1)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 152 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
0  .  .  .
j  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
```

```
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .

(1000::2, ff13::1, rpt)
RP: 4949::4949
RPF nbr: fe80::2d0:f8ff:feee:8c1f
RPF idx: GigabitEthernet 0/24
Upstream State: RPT NOT JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Pruned
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Outgoing
```

```
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .

(1000::2, ff14::1)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 76 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
0  .  .
j  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
```

```
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .

(1000::2, ff14::1, rpt)
RP: 5050::5050
RPF nbr: fe80::274:9cff:feee:f49f
RPF idx: GigabitEthernet 0/23
Upstream State: RPT NOT JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Pruned
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Outgoing
```

```
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

(1000::2, ff15::1)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: NOT JOINED
kat expires in 32 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .

(1000::2, ff15::1, rpt)
RP: 5050::5050
RPF nbr: fe80::274:9cff:feee:f49f
RPF idx: GigabitEthernet 0/23
Upstream State: RPT NOT JOINED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
Pruned
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . 
 . . .
Outgoing
```

```
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceA#
```

The routing table information on device B is as follows (only key information is displayed):

```
DeviceB> enable
DeviceB# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 2
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 1
REG Entries: 0

(*, ff13::1)
RP: 4949::4949
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
FCR:

(1000::2, ff13::1)
RPF nbr: fe80::2d0:f8ff:fe22:358d
RPF idx: GigabitEthernet 0/31
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 18 seconds
kat expires in 207 seconds

(1000::2, ff13::1, rpt)
RP: 4949::4949
```

```
RPF nbr: ::
RPF idx: None
Upstream State: PRUNED

(*, ff14::1)
RP: 5050::5050
RPF nbr: fe80::274:9cff:feee:f49f
RPF idx: GigabitEthernet 0/32
Upstream State: JOINED
jt_timer expires in 15 seconds
FCR:
Source: 1000::2
KAT timer running, 135 seconds remaining
 Packet count 1

DeviceB#
```

The routing table information on device C is as follows (only key information is displayed):

```
DeviceC> enable
DeviceC# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 2
(S,G) Entries: 2
(S,G,rpt) Entries: 2
FCR Entries: 1
REG Entries: 0

(*, ff13::1)
RP: 4949::4949
RPF nbr: fe80::2d0:f8ff:feee:8c1f
RPF idx: GigabitEthernet 0/20
Upstream State: JOINED
jt_timer expires in 40 seconds
FCR:
Source: 1000::2

 KAT timer running, 100 seconds remaining
 Packet count 1

(*, ff14::1)
RP: 5050::5050
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
FCR:
```

```
(1000::2, ff14::1)
RPF nbr: fe80::2d0:f8ff:fe22:358d
RPF idx: GigabitEthernet 0/21
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 40 seconds
kat expires in 208 seconds

(1000::2, ff14::1, rpt)
RP: 5050::5050
RPF nbr: ::
RPF idx: None
Upstream State: PRUNED

(1000::2, ff15::1)
RPF nbr: fe80::2d0:f8ff:fe22:358d
RPF idx: GigabitEthernet 0/21
SPT bit: 0
Upstream State: NOT JOINED
kat expires in 210 seconds

(1000::2, ff15::1, rpt)
RP: 5050::5050
RPF nbr: ::
RPF idx: None
Upstream State: RPT NOT JOINED

DeviceC#
```

The routing table information on device E is as follows (only key information is displayed):

```
DeviceE> enable
DeviceE# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 1
REG Entries: 0

(*, ff13::1)
RP: 4949::4949
RPF nbr: fe80::274:9cff:feee:f49f
RPF idx: GigabitEthernet 0/7
Upstream State: JOINED
jt_timer expires in 22 seconds
FCR:
```

```
Source: 1000::2
KAT timer running, 172 seconds remaining
 Packet count 1

DeviceE#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ipv6 address 1001::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim bsr-border
!
interface GigabitEthernet 0/21
 no switchport
 ipv6 address 1000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/23
 no switchport
 ipv6 address 3000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/24
 no switchport
 ipv6 address 2000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim rp-address 5050::5050
!
```

- Device B configuration file

```
hostname DeviceB
!
ipv6 access-list mcast-ipv6-list
```

```
 10 permit ipv6 any FF13::/64
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/30
 no switchport
 ipv6 address 8000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/31
 no switchport
 ipv6 address 2000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/32
 no switchport
 ipv6 address 5000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface Loopback 49
 ipv6 address 4949::4949/128
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
Ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim rp-address 5050::5050
ipv6 pim bsr-candidate Loopback 49
ipv6 pim rp-candidate Loopback 49 group-list mcast-ipv6-list
!
```

- Device C configuration file

```
hostname DeviceC
!
ipv6 access-list mcast-ipv6-list
 10 permit ipv6 any FF14::/64
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/19
 no switchport
 ipv6 address 6000::1/64
 ipv6 ospf 4949 area 0
```

```
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/20
 no switchport
 ipv6 address 5000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/21
 no switchport
 ipv6 address 3000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/22
 no switchport
 ip address 10.100.4.1 255.255.255.0
 ipv6 address 4000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface Loopback 50
 ipv6 address 5050::5050/128
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim rp-address 5050::5050
ipv6 pim bsr-candidate Loopback 50
ipv6 pim rp-candidate Loopback 50 group-list mcast-ipv6-list
!
```

- Device D configuration file

```
hostname DeviceD
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/6
 no switchport
 ipv6 address 7000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/7
 no switchport
```

```
 ipv6 address 6000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim rp-address 5050::5050
!
```

- Device E configuration file

```
hostname DeviceE
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/6
 no switchport
 ipv6 address 9000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/7
 no switchport
 ipv6 address 4000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim rp-address 5050::5050
!
```

7. Common Errors

- The multicast routing function is not enabled on multicast devices.
- The multicast function is not enabled on any interface.
- No BSR border is configured between PIM-SMv6 domains.
- No RP is configured.
- No static RP is configured on a multicast device, or the configured static RP on this multicast device is not consistent with the configuration on other multicast devices.
- C-RPs are configured, but no C-BSR is configured.
- Static RP, C-RP or C-BSR is unreachable via unicast routes.

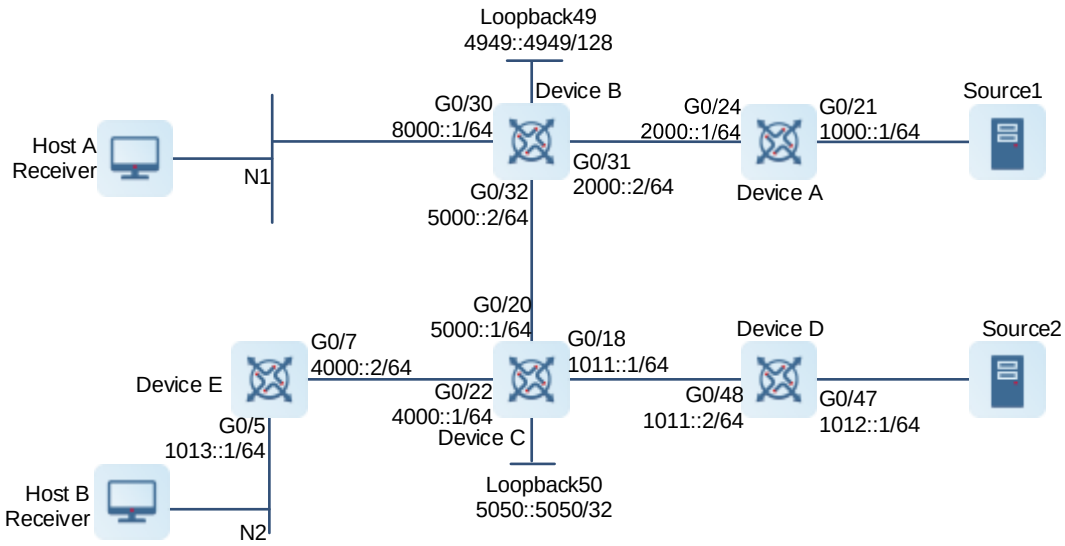
1.13.2 Configuring Basic Functions of PIM-SMv6 in the SSM Model

1. Requirements

As shown in Figure 1-6, the PIM-SMv6 protocol is enabled on multicast devices to provide SSM services for hosts in N1 and N2 so that the hosts can receive multicast data from specified multicast sources to the multicast group that the hosts join, for example, video-on-demand.

2. Topology

Figure 1-6 PIM-SMv6 Multicast Network Topology in the SSM Model



3. Notes

- Configure IPv6 addresses and unicast routing protocols for multicast devices. The PIMv6 protocol in a multicast domain depends on unicast routing protocols. Normal communication of unicast routing lays a foundation of multicast routing. Ensure that each PIMv6 node is reachable via unicast routes.
- Enable the multicast function on all multicast devices. Enabling the multicast function is a prerequisite of PIM-SMv6 configuration.
- Enable the basic functions of PIM-SMv6 on all interfaces of the multicast devices. The other functions of PIM-SMv6 can be enabled only after the basic functions of PIM-SMv6 are enabled.
- Enable the MLD function on the interface connected to hosts and set the MLD version to 2 so that the hosts can join or leave a multicast group by sending MLD messages based on the specified source. The multicast devices acting as leaf nodes maintain group membership based on the MLD protocol.
- Configure the same address range of SSM on all multicast devices. The SSM services provided by the multicast devices in the PIM-SMv6 domain are dedicated to specified groups, which realizes multicast controllability.

4. Procedure

(1) Configure IP addresses and enable unicast routing protocols on interfaces of different devices.

Configure IPv6 addresses and enable the OSPFv6 unicast routing protocol on interfaces of device A.

```
DeviceA> enable
DeviceA# config terminal
DeviceA(config)# interface GigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# no switchport
DeviceA(config-if-GigabitEthernet 0/21)# ipv6 address 1000::1/64
DeviceA(config-if-GigabitEthernet 0/21)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/21)# exit
DeviceA(config)# interface GigabitEthernet 0/24
DeviceA(config-if-GigabitEthernet 0/24)# no switchport
DeviceA(config-if-GigabitEthernet 0/24)# ipv6 address 2000::1/64
DeviceA(config-if-GigabitEthernet 0/24)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/24)# exit
```

Configure IPv6 addresses and enable the OSPFv6 unicast routing protocol on interfaces of device B.

```
DeviceB> enable
DeviceB# config terminal
DeviceB(config)# interface GigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# no switchport
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 address 8000::1/64
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 ospf 4949 area 0
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface GigabitEthernet 0/31
DeviceB(config-if-GigabitEthernet 0/31)# no switchport
DeviceB(config-if-GigabitEthernet 0/31)# ipv6 address 2000::2/64
DeviceB(config-if-GigabitEthernet 0/31)# ipv6 ospf 4949 area 0
DeviceB(config-if-GigabitEthernet 0/31)# exit
DeviceB(config)# interface GigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# no switchport
DeviceB(config-if-GigabitEthernet 0/32)# ipv6 address 5000::2/64
DeviceB(config-if-GigabitEthernet 0/32)# ipv6 ospf 4949 area 0
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface Loopback 49
DeviceB(config-if-Loopback 49)# ipv6 address 4949::4949/128
DeviceB(config-if-Loopback 49)# ipv6 ospf 4949 area 0
DeviceB(config-if-Loopback 49)# exit
```

Configure IPv6 addresses and enable the OSPFv6 unicast routing protocol on interfaces of device C.

```
DeviceC> enable
DeviceC# config terminal
DeviceC(config)# interface GigabitEthernet 0/18
DeviceC(config-if-GigabitEthernet 0/18)# no switchport
DeviceC(config-if-GigabitEthernet 0/18)# ipv6 address 1011::1/64
DeviceC(config-if-GigabitEthernet 0/18)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/18)# exit
DeviceC(config)# interface GigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# no switchport
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 address 5000::1/64
```

```
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface GigabitEthernet 0/22
DeviceC(config-if-GigabitEthernet 0/22)# no switchport
DeviceC(config-if-GigabitEthernet 0/22)# ipv6 address 4000::1/64
DeviceC(config-if-GigabitEthernet 0/22)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/22)# exit
DeviceC(config)# interface Loopback 50
DeviceC(config-if-Loopback 50)# ipv6 address 5050::5050/128
DeviceC(config-if-Loopback 50)# ipv6 ospf 4949 area 0
DeviceC(config-if-Loopback 50)# exit
```

Configure IPv6 addresses and enable the OSPFv6 unicast routing protocol on interfaces of device D.

```
DeviceD> enable
DeviceD# config terminal
DeviceD(config)# interface GigabitEthernet 0/47
DeviceD(config-if-GigabitEthernet 0/47)# no switchport
DeviceD(config-if-GigabitEthernet 0/47)# ipv6 address 1012::1/64
DeviceD(config-if-GigabitEthernet 0/47)#  ipv6 ospf 4949 area 0
DeviceD(config-if-GigabitEthernet 0/47)# exit
DeviceD(config)# interface GigabitEthernet 0/48
DeviceD(config-if-GigabitEthernet 0/48)# no switchport
DeviceD(config-if-GigabitEthernet 0/48)# ipv6 address 1011::2/64
DeviceD(config-if-GigabitEthernet 0/48)# ipv6 ospf 4949 area 0
DeviceD(config-if-GigabitEthernet 0/48)# exit
```

Configure IPv6 addresses and enable the OSPFv6 unicast routing protocol on interfaces of device E.

```
DeviceE> enable
DeviceE# config terminal
DeviceE(config)# interface GigabitEthernet 0/7
DeviceE(config-if-GigabitEthernet 0/7)# no switchport
DeviceE(config-if-GigabitEthernet 0/7)# ipv6 address 4000::2/64
DeviceE(config-if-GigabitEthernet 0/7)# ipv6 ospf 4949 area 0
DeviceE(config-if-GigabitEthernet 0/7)# exit
DeviceE(config)# interface GigabitEthernet 0/5
DeviceE(config-if-GigabitEthernet 0/5)# no switchport
DeviceE(config-if-GigabitEthernet 0/5)# ipv6 address 1013::1/64
DeviceE(config-if-GigabitEthernet 0/5)# ipv6 ospf 4949 area 0
DeviceE(config-if-GigabitEthernet 0/5)# exit
```

(2) Enable the multicast and PIM-SMv6 functions on all multicast devices, and enable the MLD function on all multicast devices connected to hosts.

Enable the IPv6 multicast and PIM-SMv6 functions on device A.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/21
DeviceA(config-if-GigabitEthernet 0/21)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/21)# exit
```

```
DeviceA(config)# interface GigabitEthernet 0/24
DeviceA(config-if-GigabitEthernet 0/24)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/24)# exit
```

Enable the IPv6 multicast, PIM-SMv6, and MLD functions on device B, and set the MLD version to 3.

```
DeviceB(config)# ipv6 multicast-routing
DeviceB(config)# interface GigabitEthernet 0/30
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/30)# ipv6 mld version 2
DeviceB(config-if-GigabitEthernet 0/30)# exit
DeviceB(config)# interface GigabitEthernet 0/31
DeviceB(config-if-GigabitEthernet 0/31)# ipv6 pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/31)# exit
DeviceB(config)# interface GigabitEthernet 0/32
DeviceB(config-if-GigabitEthernet 0/32)# ipv6 pim sparse-mode
DeviceB(config-if-GigabitEthernet 0/32)# exit
DeviceB(config)# interface Loopback 49
DeviceB(config-if-Loopback 49)# ipv6 pim sparse-mode
DeviceB(config-if-Loopback 49)# exit
```

Enable the IPv6 multicast and PIM-SMv6 functions on device C.

```
DeviceC(config)# ipv6 multicast-routing
DeviceC(config)# interface GigabitEthernet 0/18
DeviceC(config-if-GigabitEthernet 0/18)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/18)# exit
DeviceC(config)# interface GigabitEthernet 0/20
DeviceC(config-if-GigabitEthernet 0/20)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/20)# exit
DeviceC(config)# interface GigabitEthernet 0/22
DeviceC(config-if-GigabitEthernet 0/22)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/22)# exit
DeviceC(config)# interface Loopback 50
DeviceC(config-if-Loopback 50)# ipv6 pim sparse-mode
DeviceC(config-if-Loopback 50)# exit
DeviceC(config)#
```

Enable the IPv6 multicast and PIM-SMv6 functions on device D.

```
DeviceD(config)# ipv6 multicast-routing
DeviceD(config)# interface GigabitEthernet 0/47
DeviceD(config-if-GigabitEthernet 0/47)# ipv6 pim sparse-mode
DeviceD(config-if-GigabitEthernet 0/47)# exit
DeviceD(config)# interface GigabitEthernet 0/48
DeviceD(config-if-GigabitEthernet 0/48)# ipv6 pim sparse-mode
DeviceD(config-if-GigabitEthernet 0/48)# exit
```

Enable the IPv6 multicast, PIM-SMv6, and MLD functions on Device E, and set the MLD version to 3.

```
DeviceE(config)# ipv6 multicast-routing
DeviceE(config)# interface GigabitEthernet 0/7
```

```
DeviceE(config-if-GigabitEthernet 0/7)# ipv6 pim sparse-mode
DeviceE(config-if-GigabitEthernet 0/7)# exit
DeviceE(config)# interface GigabitEthernet 0/5
DeviceE(config-if-GigabitEthernet 0/5)# ipv6 mld version 2
DeviceE(config-if-GigabitEthernet 0/5)# ipv6 pim sparse-mode
DeviceE(config-if-GigabitEthernet 0/5)# exit
```

(3) Enable the SSM function and configure an address range of multicast groups on all multicast devices.

Set the address range of an SSM multicast group to FF33::/64 on device A.

```
DeviceA(config)# ipv6 access-list ipv6-ssm-list
DeviceA(config-ipv6-acl)# permit ipv6 any FF33::/64
DeviceA(config-ipv6-acl)#exit
DeviceA(config)# ipv6 pim ssm range ipv6-ssm-list
```

Set the address range of an SSM multicast group to FF33::/64 on device B.

```
DeviceB(config)# ipv6 access-list ipv6-ssm-list
DeviceB(config-ipv6-acl)# permit ipv6 any FF33::/64
DeviceB(config-ipv6-acl)#exit
DeviceB(config)# ipv6 pim ssm range ipv6-ssm-list
```

Set the address range of an SSM multicast group to FF33::/64 on device C.

```
DeviceC(config)# ipv6 access-list ipv6-ssm-list
DeviceC(config-ipv6-acl)# permit ipv6 any FF33::/64
DeviceC(config-ipv6-acl)#exit
DeviceC(config)# ipv6 pim ssm range ipv6-ssm-list
```

Set the address range of an SSM multicast group to FF33::/64 on device D.

```
DeviceD(config)# ipv6 access-list ipv6-ssm-list
DeviceD(config-ipv6-acl)# permit ipv6 any FF33::/64
DeviceD(config-ipv6-acl)#exit
DeviceD(config)# ipv6 pim ssm range ipv6-ssm-list
```

Set the address range of an SSM multicast group to FF33::/64 on device E.

```
DeviceE(config)# ipv6 access-list ipv6-ssm-list
DeviceE(config-ipv6-acl)# permit ipv6 any FF33::/64
DeviceE(config-ipv6-acl)#exit
DeviceE(config)# ipv6 pim ssm range ipv6-ssm-list
```

5. Verification

(1) Run the **show ipv6 pim sparse-mode interface** command to display the PIM-SMv6 running information on the interfaces of each device.

The PIM-SMv6 running information on the interfaces of device A is as follows. The PIM-SM running information on the interfaces of devices B, C, D, and E is the same.

```
DeviceA> enable
DeviceA# show ipv6 pim sparse-mode interface
Interface                          VIFindex Ver/   Nbr    DR
                                          Mode   Count  Prior
GigabitEthernet 0/21                 2       v2/S   0     1
```

```
   Address      : fe80::2d0:f8ff:fe22:358d
   Global Address: 1000::1
   DR          : this system
GigabitEthernet 0/24                 3       v2/S   1     1
   Address      : fe80::2d0:f8ff:fe22:358d
   Global Address: 2000::1
   DR          : fe80::2d0:f8ff:feee:8c1f
DeviceA#
```

(2) Run the **show ipv6 pim sparse-mode mroute** command to display the multicast routing tables of PIMv6. Host A needs to receive packets sent from the source (1000::2/64) and the source (1012::2/64) to the multicast group (FF33::100). Host B needs to receive packets sent from the source (1000::2/64) to the multicast group (FF33::100). The information output is as follows:

Run the **show ipv6 pim sparse-mode mroute** command to display the multicast routing tables of device A.

```
DeviceA> enable
DeviceA# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 0
FCR Entries: 0
REG Entries: 0

(1000::2, ff33::100)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 135 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
```

```
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Joined
0 . . .
j . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Outgoing
0 . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
```

```
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceA#
```

Run the **show ipv6 pim sparse-mode mroute** command to display the multicast routing tables of device B.

```
DeviceB> enable
DeviceB# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 2
(S,G,rpt) Entries: 0
FCR Entries: 0
REG Entries: 0

(1000::2, ff33::100)
RPF nbr: fe80::2d0:f8ff:fe22:358d
RPF idx: GigabitEthernet 0/31
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 14 seconds
kat expires in 122 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . .
i . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Joined
0 . .
j . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
Outgoing
0 . . o .
o . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 . . .
```

```
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

(1012::2, ff33::100)
RPF nbr: fe80::274:9cff:feee:f49f
RPF idx: GigabitEthernet 0/32
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 14 seconds
kat expires in 104 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0 . . . .
i . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
```

```
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceB#
```

Run the **show ipv6 pim sparse-mode mroute** command to display the multicast routing tables of device C.

```
DeviceC> enable
DeviceC# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 2
(S,G,rpt) Entries: 0
FCR Entries: 0
REG Entries: 0

(1000::2, ff33::100)
RPF nbr: fe80::2d0:f8ff:feee:8c1f
RPF idx: GigabitEthernet 0/20
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 30 seconds
kat expires in 91 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
0  .  .  .  .  .
j  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
```

```
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

(1012::2, ff33::100)
RPF nbr: fe80::2d0:f8ff:fe22:363d
RPF idx: GigabitEthernet 0/18
```

```
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 40 seconds
kat expires in 11 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
0  .  .  .
j  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
```

```
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceC#
```

Run the **show ipv6 pim sparse-mode mroute** command to display the multicast routing tables of device D.

```
DeviceE> enable
DeviceD# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 0
FCR Entries: 0
REG Entries: 0

(1012::2, ff33::100)
RPF nbr: ::
RPF idx: None
```

```
SPT bit: 1
Upstream State: JOINED
kat expires in 37 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
0  .  .
j  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
```

```
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 . .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceD#
```

Run the **show ipv6 pim sparse-mode mroute** command to display the multicast routing tables of device E.

```
DeviceE> enable
DeviceE# show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 0
FCR Entries: 0
REG Entries: 0

(1000::2, ff33::100)
RPF nbr: fe80::274:9cff:feee:f49f
RPF idx: GigabitEthernet 0/7
SPT bit: 1
Upstream State: JOINED
```

```
jt_timer expires in 24 seconds
kat expires in 54 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31
Local
0  .
i  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
3  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
4  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
5  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
6  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
7  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
2  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  .  .  .
```

```
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
Outgoing
0 .
o . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
5 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .
7 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
  . . .

DeviceE#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 access-list ipv6-ssm-list
 10 permit ipv6 any FF33::/64
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/21
 no switchport
 ipv6 address 1000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
```

```
interface GigabitEthernet 0/24
 no switchport
 ipv6 address 2000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim ssm range ipv6-ssm-list
!
```

- Device B configuration file

```
hostname DeviceB
!
ipv6 access-list ipv6-ssm-list
 10 permit ipv6 any FF33::/64
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/30
 no switchport
 ipv6 address 8000::1/64
 ipv6 ospf 4949 area 0
 ipv6 mld version 2
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/31
 no switchport
 ipv6 address 2000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/32
 no switchport
 ipv6 address 5000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface Loopback 49
 ipv6 address 4949::4949/128
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
```

```
ipv6 pim ssm range ipv6-ssm-list
!
```

- Device C configuration file

```
hostname DeviceC
!
ipv6 access-list ipv6-ssm-list
 10 permit ipv6 any FF33::/64
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/18
 no switchport
 ipv6 address 1011::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/20
 no switchport
 ipv6 address 5000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/22
 no switchport
 ipv6 address 4000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface Loopback 50
 ipv6 address 5050::5050/128
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim ssm range ipv6-ssm-list
!
```

- Device D configuration file

```
hostname DeviceD
!
ipv6 access-list ipv6-ssm-list
 10 permit ipv6 any FF33::/64
!
ipv6 multicast-routing
```

```
!
interface GigabitEthernet 0/47
 no switchport
 ipv6 address 1012::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/48
 no switchport
 ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim ssm range ipv6-ssm-list
!
```

- Device E configuration file

```
hostname DeviceE
!
ipv6 access-list ipv6-ssm-list
 10 permit ipv6 any FF33::/64
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/5
 no switchport
 ipv6 address 1013::1/64
 ipv6 ospf 4949 area 0
 ipv6 mld version 2
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/7
 no switchport
 ipv6 address 4000::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim ssm range ipv6-ssm-list
!
```

7. Common Errors

- IPv6 unicast routing is incorrectly configured.
- IPv6 multicast routing is not enabled on a multicast device.
- The SSM function is not enabled on a multicast device, or the SSM group address range on this multicast device is not consistent with the configuration on other multicast devices.
- The PIM-SMv6 function is not enabled on an interface, for example, the gateway interface connecting to hosts or a multicast source.
- The MLDv2 function is not enabled on an interface connected to hosts.

Contents

1 Configuring MLD Snooping 1
1.1 Introduction 1
1.1.2 Principles 1
1.1.3 Port Types 3
1.1.4 Working Mechanism 3
1.1.5 Protocols and Standards 4
1.2 Configuration Task Summary 4
1.3 Configuring Basic MLD Snooping Functions 5
1.3.1 Overview 5
1.3.2 Restrictions and Guidelines 5
1.3.3 Configuration Tasks 5
1.3.4 Configuring Basic MLD Snooping Functions in IVGL Mode 5
1.3.5 Configuring Basic MLD Snooping Functions in SVGL Mode 6
1.3.6 Configuring Basic MLD Snooping Functions in IVGL-SVGL Mode 7
1.4 Configuring Protocol Packet Processing Parameters 8
1.4.1 Overview 8
1.4.2 Restrictions and Guidelines 8
1.4.3 Configuration Tasks 8
1.4.4 Configuring a Static Multicast Router Port 8
1.4.5 Configuring a Static Member Port 9
1.4.6 Configuring Report Packet Suppression 10
1.4.7 Configuring Port Fast Leave 10

1.4.8 Configuring Dynamic Multicast Router Port Learning 11

1.4.9 Configuring the Aging Time for Dynamic Multicast Router Ports 11

1.4.10 Configuring the Aging Time for Dynamic Member Ports 12

1.4.11 Configuring the Maximum Response Time for Query Packets..... 12

1.5 Configuring Multicast Security Control 13

1.5.1 Overview 13

1.5.2 Prerequisites 13

1.5.3 Configuration Tasks 13

1.5.4 Configuring a Profile 13

1.5.5 Configuring Multicast Group Filtering on a Port 14

1.5.6 Configuring the Maximum Number of Multicast Groups That Can Be Dynamically Learned by a Port 15

1.5.7 Configuring Source Port Check 16

1.6 Monitoring 16

1.7 Configuration Examples..... 17

1.7.1 Configuring Basic MLD Snooping Functions in IVGL Mode..... 17

1.7.2 Configuring Basic MLD Snooping Functions in SVGL Mode 21

1.7.3 Configuring Basic MLD Snooping Functions in IVGL-SVGL Mode..... 26

1.7.4 Configuring Static Ports to Implement L2 Multicast..... 34

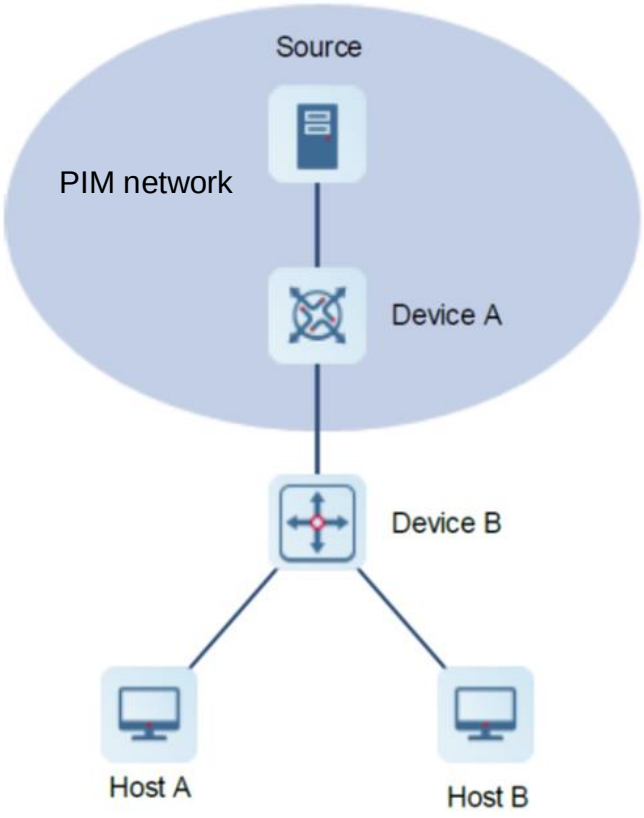
1 Configuring MLD Snooping

1.1 Introduction

Multicast Listener Discovery (MLD) snooping is a process of snooping protocol packets between an L3 multicast device and hosts to manage and control forwarding of IPv6 multicast traffic at the data link layer, implementing L2 multicast.

Generally, multicast packets need to pass through L2 switches, especially in some local area networks (LANs). As shown in Figure 1-1, the Protocol Independent Multicast (PIM) multicast device sends packets to hosts through an L2 switch. Because multicast group addresses cannot be learned on L2 devices, the packets will be broadcast in the VLAN. This wastes bandwidth and affects security. After the MLD snooping function is configured, the L2 switch can listen to MLD packets between hosts and the uplink PIM multicast device and establish L2 multicast forwarding entries to ensure that multicast data is forwarded only to specific hosts. This prevents multicast data from being broadcast in the L2 network.

Figure 1-1 Network Topology



1.1.2 Principles

MLD snooping is a basic L2 multicast function that forwards and controls multicast data at the data link layer. By listening to and analyzing protocol packets between hosts and the L3 multicast device, the L2 device running

MLD snooping establishes and maintains L2 multicast forwarding entries to ensure on-demand forwarding of multicast data at the link layer.

As shown in Figure 1-2, when MLD snooping is not configured on the L2 device, IPv6 multicast packets are broadcast in the VLAN. As shown in Figure 1-3, when MLD snooping is enabled on the L2 device, IPv6 multicast packets are forwarded only to the member hosts of the multicast group. This prevents multicast data from being broadcast in the L2 network.

Figure 1-2 Multicast Data Transmission When MLD Snooping Is Disabled

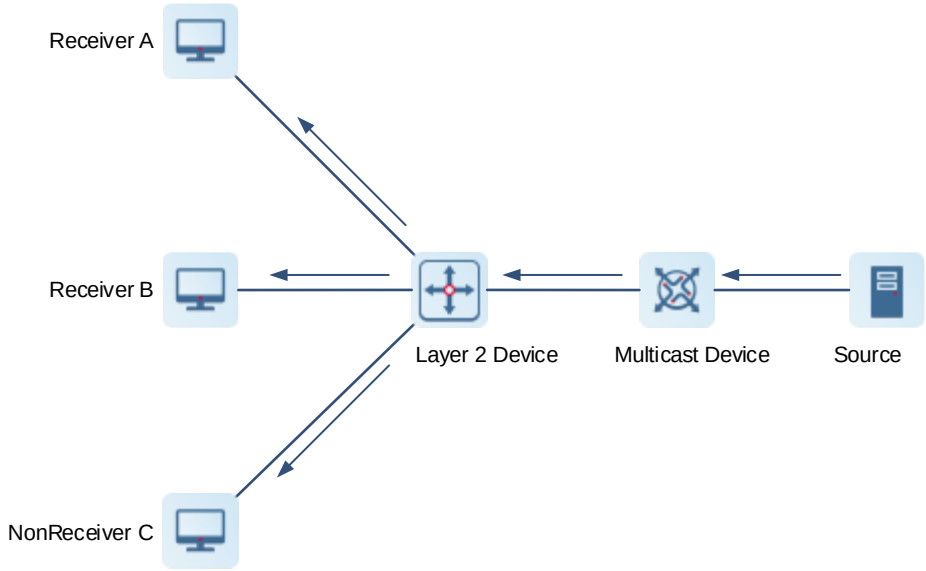
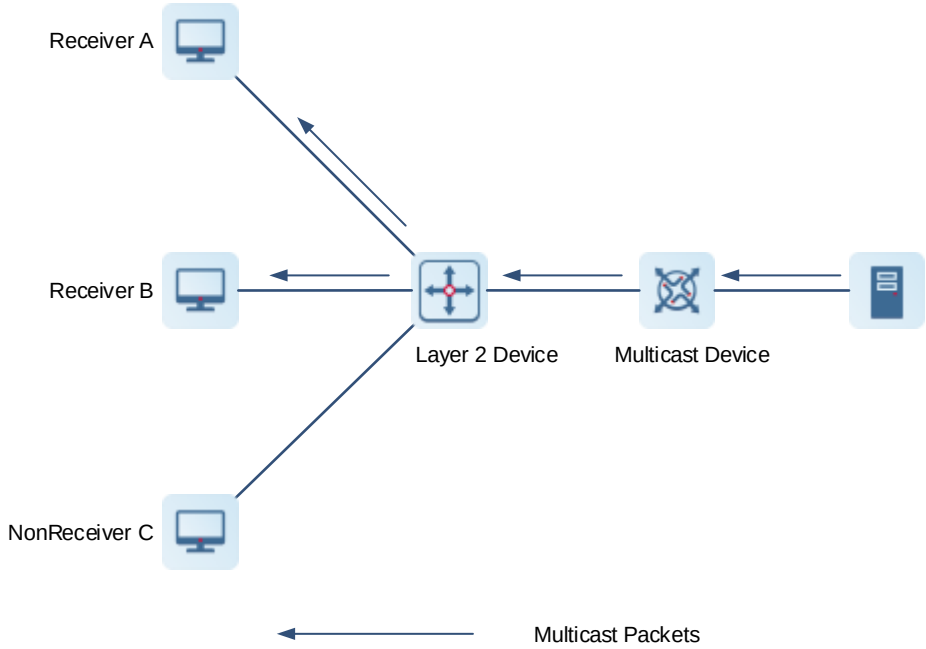


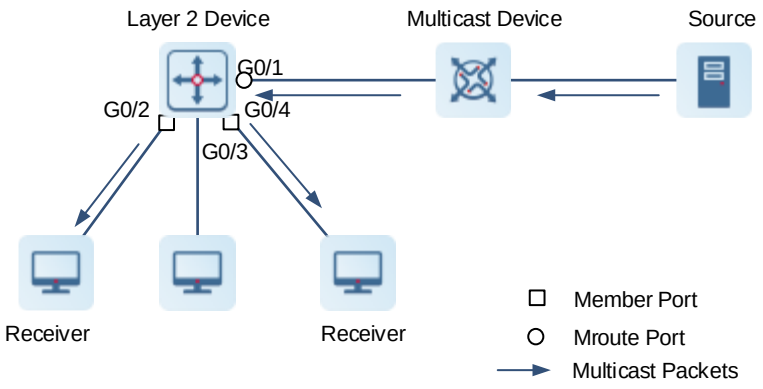
Figure 1-3 Multicast Data Transmission When MLD Snooping Is Enabled



1.1.3 Port Types

MLD snooping is enabled on a per-VLAN basis. MLD snooping ports are ports in a VLAN. The device running MLD snooping identifies ports in a VLAN as multicast router ports or member ports to manage and control forwarding of IP multicast data in the VLAN.

Figure 1-4 MLD Snooping Ports



- A multicast router port connects the L2 multicast device to an L3 multicast device, and indicates the direction of the multicast source. By listening to MLD packets, the L2 multicast device can automatically discover and maintain dynamic multicast router ports. You can also configure static multicast router ports.
- A member port connects the L2 multicast device to a host in a multicast group, and indicates the direction of a multicast group member. It is also called a listener port. By listening to MLD packets, the L2 multicast device can automatically discover and maintain dynamic member ports. You can also configure static member ports.

As shown in Figure 1-4, MLD snooping is enabled on the L2 multicast device, and the multicast data is received from a multicast router port and sent out from a member port.

1.1.4 Working Mechanism

A device running MLD snooping analyzes received MLD packets to discover and identify multicast router ports and member ports and establish and maintain MLD snooping forwarding entries. The device can identify and process the following types of MLD packets:

1. Query Packets

An L3 multicast device regularly sends an MLD general Query packet to all hosts and other multicast devices (with the address of FF02::1) in the local network segment to query the IPv6 multicast group members in this network segment. When receiving the MLD general Query packet, a multicast device forwards the packet through all ports in the VLAN except the one receiving the packet and processes the port receiving the packet as follows:

- Reset the aging timer of the port if the port is in the multicast router port list.
- Add the port to the multicast router port list if the port is not in the multicast router port list and start the aging timer of the port.
- When the L2 multicast device receives an MLD group-specific Query packet, it does not update the preceding timers.

2. Report Packets

When a member host receives a Query packet, the host will respond with a Report packet. If a host wants to join a multicast group, the host will proactively send a Report packet.

When receiving a Report packet, the device running MLD snooping forwards it to all multicast router ports in the VLAN, retrieves the address of the IPv6 multicast group that the host needs to join from the packet, and processes the port receiving the packet as follows:

- The device creates a forwarding entry for the IPv6 multicast group if no forwarding entry for the IPv6 multicast group exists, adds the port to the outbound port list as a dynamic member port, and starts the aging timer of the port.
- The device adds the port to the outbound port list as a dynamic member port and starts its aging timer if the forwarding entry of the IPv6 multicast group exists but the port is not contained in the outbound port list.
- The device resets the aging timer of the port if the forwarding entry of the IPv6 multicast group exists and the port is contained in the outbound port list.

3. Leave Packets

When a host leaves an IPv6 multicast group, it sends an MLD Leave packet (with the address of FF02::2) to notify the multicast device. When receiving a Leave packet, the device running MLD snooping performs the following actions in the VLAN:

- The device forwards the Leave packet through all multicast router ports.
- If the port receiving the Leave packet is a dynamic member port and the fast leave function is configured, the device immediately deletes the port from the MLD snooping forwarding entry of the corresponding multicast group. The port is no longer used as a dynamic member port of the group.
- If the port receiving the Leave packet is a dynamic member port but the fast leave function is not configured, the port status remains unchanged. When the aging timer of the port times out, the device deletes the port from the MLD snooping forwarding entry of the corresponding multicast group. The port is no longer used as a dynamic member port of the group.

1.1.5 Protocols and Standards

- RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

1.2 Configuration Task Summary

MLD snooping configuration includes the following tasks:

(1) Configuring Basic MLD Snooping Functions Select either of the following configuration tasks to configure.

- Configuring Basic MLD Snooping Functions in IVGL Mode
- Configuring Basic MLD Snooping Functions in SVGL Mode
- Configuring Basic MLD Snooping Functions in IVGL-SVGL Mode

(2) Configuring Protocol Packet Processing Parameters All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Static Multicast Router Port
- Configuring a Static Member Port

- Configuring Report Packet Suppression
- Configuring Port Fast Leave
- Configuring Dynamic Multicast Router Port Learning
- Configuring the Aging Time for Dynamic Multicast Router Ports
- Configuring the Aging Time for Dynamic Member Ports
- Configuring the Maximum Response Time for Query Packets

(3) Configuring Multicast Security Control All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Profile
- Configuring Multicast Group Filtering on a Port
- Configuring the Maximum Number of Multicast Groups That Can Be Dynamically Learned by a Port
- Configuring Source Port Check

1.3 Configuring Basic MLD Snooping Functions

1.3.1 Overview

The device running MLD snooping can provide independent or shared multicast services for user VLANs when operating in the following modes:

- Independent VLAN Group Learning (IVGL): provides independent multicast services for each user VLAN.
- Shared VLAN Group Learning (SVGL): provides shared multicast services for multiple user VLANs.
- IVGL-SVGL: provides both shared and independent multicast services for user VLANs.

1.3.2 Restrictions and Guidelines

- The SVGL mode and the IPv6 multicast function are mutually exclusive. If the IPv6 multicast function needs to be enabled on the device running MLD snooping, the device can operate only in IVGL mode.
- If the device running MLD snooping operates in SVGL or IVGL-SVGL mode, a profile must be defined to specify the multicast groups associated with the SVGL mode.

1.3.3 Configuration Tasks

Basic MLD snooping function configuration includes the following tasks. Please configure only one task.

- Configuring Basic MLD Snooping Functions in IVGL Mode
- Configuring Basic MLD Snooping Functions in SVGL Mode
- Configuring Basic MLD Snooping Functions in IVGL-SVGL Mode

1.3.4 Configuring Basic MLD Snooping Functions in IVGL Mode

1. Overview

In IVGL mode, the device running MLD snooping provides independent multicast services for each user VLAN. Multicast traffic can be forwarded only in the belonged VLAN, and hosts can request multicast traffic only in the belonged VLAN.

2. Restrictions and Guidelines

- Unless otherwise specified, you are advised to enable MLD snooping globally on all L2 access devices connecting to hosts.
- After MLD snooping is enabled globally, it takes effect to all VLANs. You can disable MLD snooping on any VLAN. When the multicast service is disabled on a VLAN, the multicast services on other VLANs are not affected.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IPv6 MLD snooping function and run the IVGL mode.

ipv6 mld snooping ivgl

MLD snooping is disabled by default.

(4) (Optional) Disable MLD snooping on a specified VLAN.

no ipv6 mld snooping vlan *vlan-id*

After MLD snooping is enabled globally, it takes effect to all VLANs by default. If MLD snooping is disabled globally, it is ineffective on all VLANs.

You can disable MLD snooping on a VLAN only after MLD snooping is enabled globally.

1.3.5 Configuring Basic MLD Snooping Functions in SVGL Mode

1. Overview

In SVGL mode, the device running MLD snooping can provide shared multicast services for multiple user VLANs. Shared multicast services are usually used to provide the same video on demand (VOD) service for users in multiple VLANs. Compared with independent multicast services, shared multicast services save bandwidth.

VLANs for shared multicast services are classified into a shared VLAN and sub VLANs. Multicast traffic of multicast groups applied in SVGL mode on the shared VLAN is forwarded from the shared VLAN to sub VLANs, and hosts on sub VLANs request multicast traffic of multicast groups applied in SVGL mode from the shared VLAN.

2. Restrictions and Guidelines

- Multicast services can be shared among VLANs. After configuring the SVGL mode, you need to configure multicast groups applied in SVGL mode.
- Shared multicast services apply only to the shared VLAN and sub VLANs and use group addresses applied in SVGL mode.

3. Prerequisites

Before configuring multicast groups associated with the SVGL mode, ensure that the corresponding profile is created and a range of multicast groups that are permitted or denied by the filter is specified. For details about profile configuration, see 1.5.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IPv6 MLD snooping function and run the SVGL mode.

ipv6 mld snooping svgl

MLD snooping is disabled by default.

(4) Configure multicast groups associated with the SVGL mode.

ipv6 mld snooping svgl profile *profile-number*

No multicast group is associated with the SVGL mode by default.

(5) (Optional) Specify a shared VLAN.

ipv6 mld snooping svgl vlan *vlan-id*

The default shared VLAN in SVGL mode is VLAN 1.

1.3.6 Configuring Basic MLD Snooping Functions in IVGL-SVGL Mode

1. Overview

The IVGL-SVGL mode is also called the hybrid mode. In IVGL-SVGL mode, the device running MLD snooping can provide both shared and independent multicast services for user VLANs.

- In the shared VLAN and sub VLANs, shared multicast services apply to the multicast traffic of multicast groups applied in SVGL mode, and independent multicast services apply to other multicast traffic.
- In other VLANs (except the shared VLAN and sub VLANs), independent multicast services are provided.

2. Restrictions and Guidelines

- After configuring the IVGL-SVGL mode, you must specify the multicast groups associated with the SVGL mode.
- When a user VLAN is configured as a shared VLAN or sub VLAN, the user VLAN enjoys both shared and independent multicast services. When a user VLAN is configured as other VLANs, it enjoys only independent multicast services.

3. Prerequisites

Before configuring multicast groups associated with the SVGL mode, ensure that the corresponding profile is created and a range of multicast groups that are permitted or denied by the filter is specified. For details about profile configuration, see 1.5.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IPv6 MLD snooping function and run the IVGL-SVGL mode.

ipv6 mld snooping ivgl-svgl

MLD snooping is disabled by default.

(4) (Optional) Specify a shared VLAN.

ipv6 mld snooping svgl vlan *vlan-id*

The default shared VLAN in SVGL mode is VLAN 1.

1.4 Configuring Protocol Packet Processing Parameters

1.4.1 Overview

By controlling protocol packet processing, an L2 multicast device can establish static or dynamic multicast forwarding entries. In addition, the device can adjust parameters to refresh dynamic multicast forwarding entries and MLD snooping membership quickly.

1.4.2 Restrictions and Guidelines

Configuring Basic MLD Snooping Functions Related configuration functions take effect only after basic MLD snooping functions are configured.

1.4.3 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Static Multicast Router Port
- Configuring a Static Member Port
- Configuring Report Packet Suppression
- Configuring Port Fast Leave
- Configuring Dynamic Multicast Router Port Learning
- Configuring the Aging Time for Dynamic Multicast Router Ports
- Configuring the Aging Time for Dynamic Member Ports
- Configuring the Maximum Response Time for Query Packets

1.4.4 Configuring a Static Multicast Router Port

1. Overview

A multicast router port is used to receive uplink multicast data and forward MLD Report and Leave packets. Static multicast router ports never age and can forward MLD Report and Leave packets to the uplink MLD querier stably.

2. Restrictions and Guidelines

- In SVGL mode, if no sub VLAN is configured, the configuration of static multicast router ports is valid only in the shared VLAN. In other VLANs, static multicast router ports can be configured but do not take effect. If sub VLANs are configured, the configuration of static multicast router ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static multicast router ports can be configured but do not take effect.
- In SVGL-IVGL mode, if no sub VLAN is configured, the configuration of static multicast router ports is valid in all VLANs. If sub VLANs are configured, the configuration of static multicast router ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static multicast router ports can be configured but do not take effect.
- In IVGL mode, the configuration of static multicast router ports is valid in all VLANs.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static multicast router port.

ipv6 mld snooping vlan *vlan-id* **mrouter interface** *interface-type interface-number*

No static multicast router port is configured by default.

1.4.5 Configuring a Static Member Port

1. Overview

When a member port connecting to a member host is configured as a static member port, the host can receive multicast traffic from the specified multicast group no matter whether the host joins the multicast group. Static member ports never age.

2. Restrictions and Guidelines

- In SVGL mode, if no sub VLAN is configured, the configuration of static member ports is valid only in the shared VLAN. In other VLANs, static member ports can be configured but do not take effect. If sub VLANs are configured, the configuration of static member ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static member ports can be configured but do not take effect.
- In SVGL-IVGL mode, if no sub VLAN is configured, the configuration of static member ports is valid in all VLANs. If sub VLANs are configured, the configuration of static member ports is valid in the shared VLAN and non-sub VLANs. In sub VLANs, static member ports can be configured but do not take effect.
- In IVGL mode, the configuration of static member ports is valid in all VLANs.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static member port.

ipv6 mld snooping vlan *vlan-id* **static** *ipv6-group-address* **interface** *interface-type interface-number*

No static member port is configured by default.

1.4.6 Configuring Report Packet Suppression

1. Overview

MLD Query and Report packets are exchanged periodically to maintain the group membership. When many hosts in a network join the same multicast group, many MLD packets will be sent to the MLD multicast device, which wastes network bandwidth and affects the performance of the MLD multicast device. Report packet suppression can optimize this situation.

When Report packet suppression is configured, the MLD multicast device forwards only the first Report packet from a specific VLAN for a multicast group to the multicast router port and suppresses subsequent Report packets for the same multicast group during one query interval. This function helps reduce the number of packets in the network.

2. Restrictions and Guidelines

Only MLDv1 Report packets can be suppressed, and MLDv2 Report packets cannot be suppressed.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure Report packet suppression.

ipv6 mld snooping suppression enable

Report packet suppression is disabled by default.

1.4.7 Configuring Port Fast Leave

1. Overview

When the port fast leave function is enabled and a port receives a Leave packet (including the MLDv1 Leave packet and MLDv2 Report packet of the INCLUDE type without carrying any source address), the port is directly deleted from the member port list of the corresponding multicast forwarding entry. When receiving group-specific Query packets and multicast data, the device does not forward the packets to this port.

2. Restrictions and Guidelines

The port fast leave function is applicable when only one host is connected to each port. This function helps save bandwidth and resources.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the port fast leave function.

ipv6 mld snooping fast-leave enable

The port fast leave function is disabled by default.

1.4.8 Configuring Dynamic Multicast Router Port Learning

1. Overview

In some test scenarios, a user host may send Query packets and PIMv6 neighbor messages. When the L2 device receives such Query packets or PIM neighbor messages, the L2 device will set the port receiving the packets as a dynamic multicast router port. All multicast packets in the VLAN will be forwarded to this port, and the host receives a large number of useless multicast packets. In addition, Query packets and PIMv6 neighbor messages sent by user hosts may affect the status of the L3 multicast routing protocol, such as the querier and designated router (DR) election. In this case, you can disable dynamic multicast router port learning to resolve this problem and improve network security.

2. Restrictions and Guidelines

Disabling dynamic multicast router port learning and enabling a static multicast router port do not affect each other.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure dynamic multicast router port learning.

ipv6 mld snooping [**vlan** *vlan-id*] **mrouter learn**

Dynamic multicast router port learning is enabled by default.

1.4.9 Configuring the Aging Time for Dynamic Multicast Router Ports

1. Overview

A multicast router port is used to receive uplink multicast data and forward MLD Report and Leave packets. After enabling MLD snooping, an L2 device can dynamically learn multicast router ports to forward multicast packets for the unplink device. If a dynamic multicast router port does not receive a Query packet or neighbor message from the uplink device within the aging time due to unstable network or packet congestion, the L2 device will delete the dynamic multicast router port, which may cause multicast data interruption.

2. Restrictions and Guidelines

You can adjust the aging time of dynamic multicast router ports based on the network load. When the network load is heavy, set the aging time to a larger value. A too short aging time may cause dynamic multicast router ports to be added and deleted frequently, resulting in data interruption.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the aging time for dynamic multicast router ports.

ipv6 mld snooping dyn-mr-aging-time *dynamic-mroute-aging-time*

The default aging time of dynamic multicast router ports is 300s.

1.4.10 Configuring the Aging Time for Dynamic Member Ports

1. Overview

When the device running MLD snooping receives an MLD Join packet from a host to join an IP multicast group, the device adds the port receiving the packet to the member port list and sets an aging time for the port. If the port is already in the member port list, the device resets the aging timer of the port. If the timer times out, it is deemed that no user host receives multicast packets through this port, and the multicast device deletes the port from the MLD snooping member port list.

2. Restrictions and Guidelines

- You can adjust the aging time of dynamic member ports based on the network load. When the network load is heavy, set the aging time to a larger value. A too short aging time may cause dynamic member ports to be added and deleted frequently, resulting in data interruption.
- After this command is configured, the aging timer value of dynamic member ports is *host-aging-time* for subsequent MLD Join packets. The aging time takes effect immediately after configuration and the started member port timers are updated.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the aging time for dynamic member ports.

ipv6 mld snooping host-aging-time *host-aging-time*

The default aging time of dynamic member ports is 260s.

1.4.11 Configuring the Maximum Response Time for Query Packets

1. Overview

When hosts in the directly-connected network segment of the device serving as the MLD snooping querier receive a Query packet from the device, the hosts need to return a Report packet within the maximum response time. This function allows you to configure the maximum response time for Query packets on the device. If no host returns a Report packet within the maximum response time, the device considers that no group member exists in the directly-connected network segment and deletes the group information.

2. Restrictions and Guidelines

- When receiving an MLD general Query packet, the multicast device will update the aging timers of all member ports. The timer time is the maximum response time for Query packets. After the timer expires, the device regards that no group member receives multicast traffic through a port and deletes the port from the MLD snooping forwarding table.
- When receiving an MLD group-specific Query packet, the multicast device will start the aging timers of all member ports of the specific group. The timer time is the maximum response time for Query packets. After the timer expires, the device regards that no group member receives multicast traffic through a port and deletes the port from the MLD snooping forwarding table.
- For MLDv2 group-specific Query packets, the multicast device does not update the timers.
- The configured response time for Query packets takes effect when the next Query packet is received.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum response time for Query packets.

ipv6 mld snooping query-max-response-time *query-max-response-time*

The maximum response time for Query packets is 10s by default.

1.5 Configuring Multicast Security Control

1.5.1 Overview

After multicast security control is configured, the device running MLD snooping can control the multicast service scope and load to prevent invalid multicast traffic and improve L2 multicast network security.

1.5.2 Prerequisites

Configuring Basic MLD Snooping Functions

1.5.3 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Profile
- Configuring Multicast Group Filtering on a Port
- Configuring the Maximum Number of Multicast Groups That Can Be Dynamically Learned by a Port
- Configuring Source Port Check

1.5.4 Configuring a Profile

1. Overview

A profile is used to define a range of multicast groups that permit or deny user access for reference by other functions.

- When the SVGL mode is enabled, a profile is used to define a range of multicast groups applied in SVGL mode.
- When multicast filtering is configured on a port, a profile is used to define a range of multicast groups that permit or deny user access through the port.
- When multicast filtering is configured on a VLAN, a profile is used to define a range of multicast groups that permit or deny user access on the VLAN.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a profile.

ipv6 mld profile *profile-number*

No profile is created by default.

(4) Define a range of multicast groups for a profile.

range *low-ipv6-address* [*high-ipv6-address*]

No multicast group range is defined for a profile by default.

Multiple multicast group ranges can be configured at the same time. If two multicast group ranges overlap, the ranges will be merged automatically.

(5) Configure the filtering action for a profile. The configuration steps below are mutually exclusive. Please configure only one task.

- Set the filtering action of a profile to Deny.

  deny

  If only the Deny action is configured and no multicast group range is configured, no group is denied. The effect is the same as permitting all groups.

- Set the filtering action of a profile to Permit.

  permit

  If only the Permit action is configured and no multicast group range is configured, no group is permitted. The effect is the same as denying all groups.

The Deny action is performed for a profile by default.

1.5.5 Configuring Multicast Group Filtering on a Port

1. Overview

Generally, the device running ports can join any multicast group. By configuring a range of multicast groups that permit or deny user access, you can customize the multicast service scope for users to guarantee the interest of operators and prevent invalid multicast traffic.

2. Restrictions and Guidelines

By applying a profile to a port, you can restrict the multicast groups that users can join on the port.

3. Prerequisites

Before configuring a range of multicast groups for a profile, ensure that the corresponding profile is created and a range of multicast groups that are permitted or denied by the filter is specified. For details about profile configuration, see 1.5.4 Configuring a Profile.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure multicast group filtering on a port.

ipv6 mld snooping filter *profile-number*

The multicast group filtering function is disabled on a port by default.

1.5.6 Configuring the Maximum Number of Multicast Groups That Can Be Dynamically Learned by a Port

1. Overview

If too much multicast traffic is requested concurrently, the multicast device will be severely burdened. Configuring the maximum number of multicast groups allowed for concurrent request can guarantee the bandwidth. You can limit the number of multicast groups allowed for concurrent request on a port.

2. Restrictions and Guidelines

Only dynamically learned multicast groups on a port are counted. Statically configured multicast groups are excluded.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum number of multicast groups that can be dynamically learned by a port.

ipv6 mld snooping max-groups *max-groups-number*

The maximum number of multicast groups that can be dynamically learned by a port is 64,000 by default.

1.5.7 Configuring Source Port Check

1. Overview

The source port check function restricts users to receive only multicast traffic on multicast router ports to prevent users from sending invalid multicast traffic.

- After the source port check function is enabled, only multicast traffic received on multicast router ports is valid. Multicast traffic received on other ports is invalid and will be discarded.
- When the source port check function is disabled, multicast traffic received on any port is valid.

2. Restrictions and Guidelines

- To restrict users to receive multicast traffic only on multicast router ports, configure this function.
- If no multicast router port exists after the source port check function is enabled, the device will discard received multicast traffic.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure source port check.

ipv6 mld snooping source-check port

Source port check is disabled by default.

1.6 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

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

Table 1-1 Monitoring

Command	Purpose
clear ipv6 mld snooping gda-table	Clears MLD snooping multicast forwarding entries.
clear ipv6 mld snooping statistics	Clears MLD snooping statistics.
show ipv6 mld snooping	Displays the current MLD snooping mode.
show ipv6 mld snooping gda-table	Displays MLD snooping forwarding entries.

Command	Purpose
show ipv6 mld snooping statistics	Displays MLD snooping statistics.
show ipv6 mld snooping mrouter	Displays MLD snooping multicast router ports.
show ipv6 mld snooping interfaces [*interface-type interface-name*]	Displays MLD snooping interface information, interface filtering profile, and maximum number of multicast groups that can be dynamically learned by a port.
show ipv6 mld snooping vlan *vlan-id*	Displays multicast information about a single VLAN, on which MLD snooping is configured.
show ipv6 mld profile *profile-number*	Displays an MLD profile.

1.7 Configuration Examples

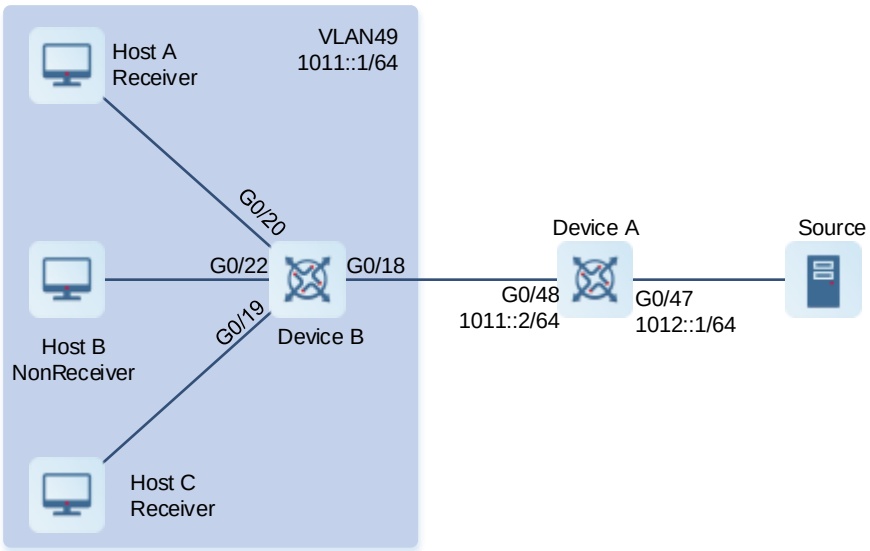
1.7.1 Configuring Basic MLD Snooping Functions in IVGL Mode

1. Requirements

In the multicast network shown in Figure 1-5, the router (Device A) connects to the user network through the switch (Device B), and MLD snooping is run on Device A. The multicast source sends data to multicast group FF14::10. There are three hosts (Host A, Host B, and Host C) in the network. Host A and Host C join multicast group FF14::10. Only Host A and Host B can receive multicast data that the multicast source sends to multicast group FF14::10.

2. Topology

Figure 1-5 Topology of Basic MLD Snooping Functions in IVGL Mode



3. Notes

Configure basic MLD snooping functions on Device B.

- Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and PIM-SMv6 related functions on Device A.
- Enable MLD snooping and run the IVGL mode on Device B.

4. Procedure

(1) Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IPv6 address and unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 address 1012::1/64
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# no switchport
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 address 1011::2/64
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ipv6 router ospf 4949
DeviceA(config-router)# exit
```

Configure the IPv6 address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan 49
DeviceB(config-vlan)# exit
DeviceB(config)# interface vlan 49
DeviceB(config-if-VLAN 49)# ipv6 address 1011::1/64
DeviceB(config-if-VLAN 49)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 49)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/22
```

```
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# ipv6 router ospf 4949
DeviceB(config-router)# exit
```

(2) Enable multicast routing and PIM-SMv6 related functions on Device A.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ipv6 pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ipv6 pim rp-candidate GigabitEthernet 0/47
```

(3) Enable MLD snooping and run the IVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld snooping ivgl
```

5. Verification

Send packets from the multicast source (1012::2) to multicast group G (FF14::10). Enable Host A and Host C to join G.

Run the **show ipv6 mld snooping gda-table** command on Device B to display the MLD snooping forwarding entry and check whether the member port list contains only GigabitEthernet 0/19 and GigabitEthernet 0/20.

```
DeviceB> enable
DeviceB# show ipv6 mld snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, FF14::10, 49):
  VLAN(49) 3 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/19(M)
    GigabitEthernet 0/20(DM)

DeviceB#
```

Run the **show ipv6 mld snooping** command on Device B and check whether the MLD snooping working mode is IVGL.

```
DeviceB# show ipv6 mld snooping
MLD-snooping mode: IVGL
Source port check: Disable
MLD Fast-Leave: Disable
```

```
MLD Report suppress: Disable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)
MLD Snooping version: 1
MLD Tunnel: Disable

vlan 49
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/47
 no switchport
 ipv6 address 1012::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/48
 no switchport
 ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 pim bsr-candidate GigabitEthernet 0/47
ipv6 pim rp-candidate GigabitEthernet 0/47
!
```

- Device B configuration file

```
hostname DeviceB
!
vlan range 1,49
!
interface GigabitEthernet 0/18
 switchport access vlan 49
!
interface GigabitEthernet 0/19
```

```
 switchport access vlan 49
!
interface GigabitEthernet 0/20
 switchport access vlan 49
!
interface GigabitEthernet 0/22
 switchport access vlan 49
!
interface VLAN 49
 ipv6 address 1011::1/64
 ipv6 ospf 4949 area 0
!
Ipv6 mld snooping ivgl
!
```

7. Common Errors

- The working mode of MLD snooping is improper.

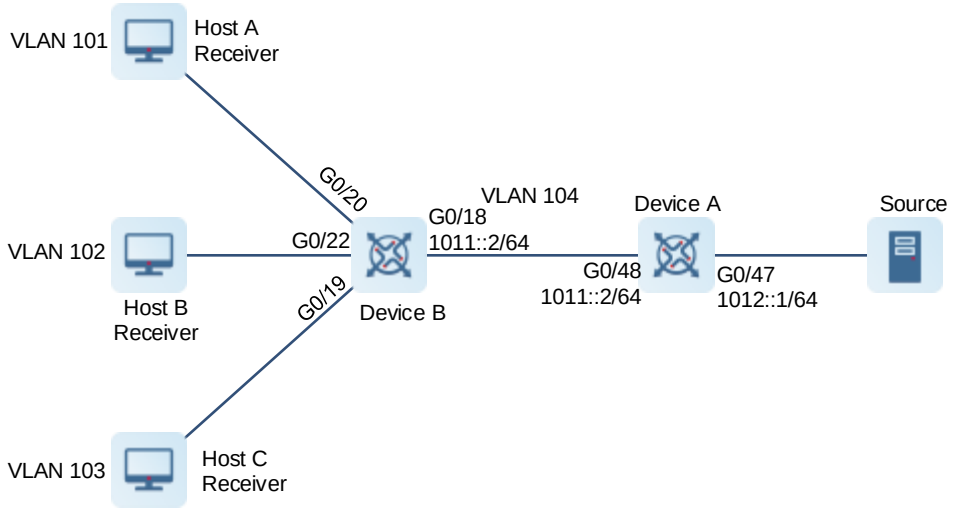
1.7.2 Configuring Basic MLD Snooping Functions in SVGL Mode

1. Requirements

In the multicast network shown in Figure 1-6, the router (Device A) connects to the user network through the switch (Device B), MLD snooping is run on Device A, and Device A directly connects to the multicast source. The multicast source sends data to multicast group FF14::10. Host A, Host B, and Host C are connected to VLAN 101, VLAN 102, and VLAN 103, respectively, and the three hosts join multicast group FF14::10. Host A, Host B, and Host C can receive multicast data that the multicast source sends to multicast group FF14::10.

2. Topology

Figure 1-6 Topology of Basic MLD Snooping Functions in SVGL Mode



3. Notes

Configure basic MLD snooping functions on Device B.

- Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and PIM-SMv6 related functions on Device A.
- Enable MLD snooping and run the SVGL mode on Device B.
- Configure the multicast groups associated with the MLD snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

4. Procedure

(1) Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IP address and unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 address 1012::1/64
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# vlan 104
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ipv6 address 1011::2/64
DeviceA(config-if-VLAN 104)# ipv6 ospf 4949 area 0
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/48)# switchport trunk native vlan 104
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ipv6 router ospf 4949
DeviceA(config-router)# exit
```

Configure the IPv6 address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan range 101-104
DeviceB(config-vlan-range)# exit
DeviceB(config)# interface VLAN 101
DeviceB(config-if-VLAN 101)# ipv6 address 1010::1/64
DeviceB(config-if-VLAN 101)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 101)# exit
DeviceB(config)# interface VLAN 102
DeviceB(config-if-VLAN 102)# ipv6 address 1020::1/64
DeviceB(config-if-VLAN 102)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 102)# exit
DeviceB(config)# interface VLAN 103
DeviceB(config-if-VLAN 103)# ipv6 address 1030::1/64
```

```
DeviceB(config-if-VLAN 103)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 103)# exit
DeviceB(config)# interface VLAN 104
DeviceB(config-if-VLAN 104)# ipv6 address 1011::2/64
DeviceB(config-if-VLAN 104)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 104)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/18)# switchport trunk native vlan 104
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 103
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 101
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 102
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# ipv6 router ospf 4949
DeviceB(config-router)# exit
```

(2) Enable multicast routing and PIM-SM related functions on Device A.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ipv6 pim sparse-mode
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# ipv6 pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ipv6 pim rp-candidate GigabitEthernet 0/47
```

(3) Enable MLD snooping and run the IVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld snooping svgl
```

(4) Configure the multicast groups associated with the MLD snooping SVGL mode on Device B and specify the shared VLAN.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld profile 1
DeviceB(config-profile)# permit
DeviceB(config-profile)# range ff13::1 ff14::fff
DeviceB(config-profile)# exit
DeviceB(config)# ipv6 mld snooping svgl profile 1
DeviceB(config)# ipv6 mld snooping svgl vlan 104
```

5. Verification

Send packets from the multicast source (1012::2) to multicast group G (FF14::10). Enable Host A, Host B, and Host C to join G.

Run the **show ipv6 mld snooping gda-table** command on Device B to display the MLD snooping forwarding entry and check whether the member port list contains GigabitEthernet 0/19, GigabitEthernet 0/20, and GigabitEthernet 0/22.

```
DeviceB> enable
DeviceB# show ipv6 mld snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, FF14::10, 104):
  VLAN(104) 1 OPORTS:
    GigabitEthernet 0/18(M)

  VLAN(101) 1 OPORTS:
    GigabitEthernet 0/20(D)

  VLAN(103) 1 OPORTS:
    GigabitEthernet 0/19(D)

  VLAN(102) 1 OPORTS:
    GigabitEthernet 0/22(D)

DeviceB#
```

Run the **show ipv6 mld snooping** command on Device B and check whether the MLD snooping working mode is SVGL.

```
DeviceB> enable
DeviceB# show ipv6 mld snooping
MLD-snooping mode: SVGL
SVGL vlan: 104
SVGL profile number: 1
Source port check: Disable
MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)
MLD Snooping version: 1
MLD Tunnel: Disable
DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
vlan 104
!
interface GigabitEthernet 0/47
 no switchport
 ipv6 address 1012::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
interface GigabitEthernet 0/48
 switchport mode trunk
 switchport trunk native vlan 104
!
interface VLAN 104
 ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode!
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim bsr-candidate GigabitEthernet 0/47
ipv6 pim rp-candidate GigabitEthernet 0/47
!
```

- Device B configuration file

```
hostname DeviceB
!
ipv6 mld profile 1
 permit
 range FF13::1 FF14::FFF
!
vlan range 1,101-104
!
interface GigabitEthernet 0/18
 switchport mode trunk
 switchport trunk native vlan 104
!
interface GigabitEthernet 0/19
 switchport access vlan 103
!
interface GigabitEthernet 0/20
 switchport access vlan 101
!
interface GigabitEthernet 0/22
```

```
 switchport access vlan 102
!
interface VLAN 101
 ipv6 address 1010::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 102
 ipv6 address 1020::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 103
 ipv6 address 1030::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 104
 ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 mld snooping svgl vlan 104
ipv6 mld snooping svgl profile 1
ipv6 mld snooping svgl
!
```

7. Common Errors

- The multicast groups associated with the SVGL mode are not configured.
- The address of the sent multicast traffic is not within the range of multicast groups associated with the SVGL mode.

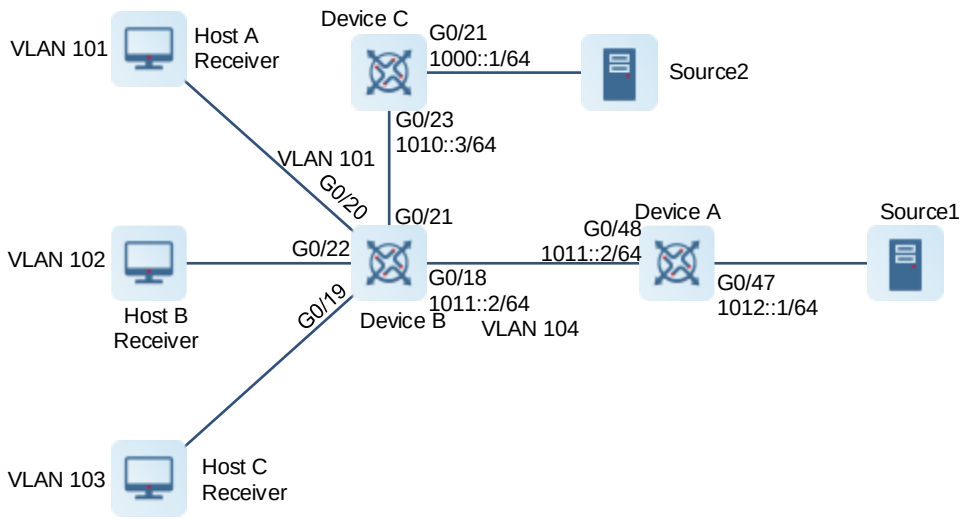
1.7.3 Configuring Basic MLD Snooping Functions in IVGL-SVGL Mode

1. Requirements

In the multicast network shown in Figure 1-7, the routers (Device A and Device C) connect to the user network through the switch (Device B), MLD snooping is run on Device A and Device C, and Device A and Device C directly connect to the multicast sources. Multicast source 1 sends data to multicast group FF14::10, and multicast source 2 sends data to multicast group FF15::11. Host A, Host B, and Host C are connected to VLAN 101, VLAN 102, and VLAN 103, respectively. Host B and Host C join multicast group FF14::10, and Host A joins multicast groups FF14::10 and FF15::11. Host B and Host C can receive multicast data that source 1 sends to multicast group FF14::10, and Host A can receive multicast data that source 1 sends to multicast group FF14::10 and multicast data that source 2 sends to multicast group FF15::11. Host A, Host B, and Host C enjoy shared multicast services, and Host A also enjoy independent multicast services.

2. Topology

Figure 1-7 Topology of Basic MLD Snooping Functions in IVGL-SVGL Mode



3. Notes

Configure basic MLD snooping functions in IVGL-SVGL mode on Device B.

- Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and PIM-SMv6 related functions on Device A and Device C.
- Enable MLD snooping and run the IVGL-SVGL mode on Device B.
- Configure the multicast groups associated with the MLD snooping SVGL mode on Device B and specify the shared VLAN and sub VLANs.

4. Procedure

(1) Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IPv6 address and unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 address 1012::1/64
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# vlan 104
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ipv6 address 1011::2/64
DeviceA(config-if-VLAN 104)# ipv6 ospf 4949 area 0
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# interface GigabitEthernet 0/48
```

```
DeviceA(config-if-GigabitEthernet 0/48)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/48)# switchport trunk native vlan 104
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ipv6 router ospf 4949
DeviceA(config-router)# exit
```

Configure the IPv6 address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan range 101-104
DeviceB(config-vlan-range)# exit
DeviceB(config)# interface VLAN 101
DeviceB(config-if-VLAN 101)# ipv6 address 1010::1/64
DeviceB(config-if-VLAN 101)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 101)# exit
DeviceB(config)# interface VLAN 102
DeviceB(config-if-VLAN 102)# ipv6 address 1020::1/64
DeviceB(config-if-VLAN 102)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 102)# exit
DeviceB(config)# interface VLAN 103
DeviceB(config-if-VLAN 103)# ipv6 address 1030::1/64
DeviceB(config-if-VLAN 103)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 103)# exit
DeviceB(config)# interface VLAN 104
DeviceB(config-if-VLAN 104)# ipv6 address 1011::2/64
DeviceB(config-if-VLAN 104)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 104)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport mode trunk
DeviceB(config-if-GigabitEthernet 0/18)# switchport trunk native vlan 104
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 103
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 101
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/21
DeviceB(config-if-GigabitEthernet 0/21)# switchport access vlan 101
DeviceB(config-if-GigabitEthernet 0/21)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 102
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# ipv6 router ospf 4949
DeviceB(config-router)# exit
```

Configure the IPv6 address and unicast routing protocol on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# no switchport
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 address 1000::1/64
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface GigabitEthernet 0/23
DeviceC(config-if-GigabitEthernet 0/23)# no switchport
DeviceC(config-if-GigabitEthernet 0/23)# ipv6 address 1010::3/64
DeviceC(config-if-GigabitEthernet 0/23)# ipv6 ospf 4949 area 0
DeviceC(config-if-GigabitEthernet 0/23)# exit
DeviceC(config)# ipv6 router ospf 4949
DeviceC(config-router)# exit
```

(2) Enable IPv6 multicast routing and PIM-SMv6 related functions on Device A and Device C.

Enable IPv6 multicast routing and PIM-SMv6 related functions on Device A.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface vlan 104
DeviceA(config-if-VLAN 104)# ipv6 pim sparse-mode
DeviceA(config-if-VLAN 104)# exit
DeviceA(config)# ipv6 pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ipv6 pim rp-candidate GigabitEthernet 0/47
```

Enable multicast routing and PIM-SMv6 related functions on Device C.

```
DeviceC(config)# ipv6 multicast-routing
DeviceC(config)# interface GigabitEthernet 0/21
DeviceC(config-if-GigabitEthernet 0/21)# no switchport
DeviceC(config-if-GigabitEthernet 0/21)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/21)# exit
DeviceC(config)# interface GigabitEthernet 0/23
DeviceC(config-if-GigabitEthernet 0/23)# ipv6 pim sparse-mode
DeviceC(config-if-GigabitEthernet 0/23)# exit
```

(3) Enable MLD snooping and run the IVGL-SVGL mode on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld snooping ivgl-svgl
```

(4) Configure the multicast groups associated with the MLD snooping SVGL mode on Device B and specify the shared VLAN.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld profile 1
DeviceB(config-profile)# permit
```

```
DeviceB(config-profile)# range ff13::1 ff14::fff
DeviceB(config-profile)# exit
DeviceB(config)# ipv6 mld snooping svgl profile 1
DeviceB(config)# ipv6 mld snooping svgl vlan 104
```

5. Verification

Run the **show ipv6 mld snooping gda-table** command on Device B to display the MLD snooping forwarding entries and check whether the member port list of entry (*, FF14::10, 104) contains GigabitEthernet 0/22, GigabitEthernet 0/20, and GigabitEthernet 0/19 and the member port list of entry (*, FF15::11, 101) contains GigabitEthernet 0/20.

```
DeviceB> enable

DeviceB# show ipv6 mld snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, FF15::11, 101):
  VLAN(101) 2 OPORTS:
    GigabitEthernet 0/20(D)
    GigabitEthernet 0/21(M)

(*, FF14::10, 104):
  VLAN(104) 1 OPORTS:
    GigabitEthernet 0/18(M)

  VLAN(103) 1 OPORTS:
    GigabitEthernet 0/19(D)

  VLAN(102) 1 OPORTS:
    GigabitEthernet 0/22(D)

  VLAN(101) 1 OPORTS:
    GigabitEthernet 0/20(D)

DeviceB#
```

Run the **show ipv6 mld snooping** command on Device B and check whether the MLD snooping working mode is IVGL-SVGL.

```
DeviceB# show ipv6 mld snooping
MLD-snooping mode: IVGL-SVGL
SVGL vlan: 104
SVGL profile number: 1
Source port check: Disable
MLD Fast-Leave: Disable
MLD Report suppress: Disable
```

```
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300(Seconds)
Dynamic Host Aging Time: 260(Seconds)
MLD Snooping version: 1
MLD Tunnel: Disable

vlan 1
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC

vlan 101
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC

vlan 102
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC

vlan 103
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC

vlan 104
-------------
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC
DeviceB#
```

6. Configuration Files

```
Device A configuration file
hostname DeviceA
!
```

```
ipv6 multicast-routing
!
vlan 104
!
interface GigabitEthernet 0/47
 no switchport
 ipv6 address 1012::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
interface GigabitEthernet 0/48
 switchport mode trunk
 switchport trunk native vlan 104
!
interface VLAN 104
ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode!
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim bsr-candidate GigabitEthernet 0/47
ipv6 pim rp-candidate GigabitEthernet 0/47
!
```

- Device B configuration file

```
hostname DeviceB
!
ipv6 mld profile 1
 permit
 range FF13::1 FF14::FFF
!
vlan range 1,101-104
!
interface GigabitEthernet 0/18
 switchport mode trunk
 switchport trunk native vlan 104
!
interface GigabitEthernet 0/19
 switchport access vlan 103
!
interface GigabitEthernet 0/20
 switchport access vlan 101
!
interface GigabitEthernet 0/21
 switchport access vlan 101
!
```

```
interface GigabitEthernet 0/22
 switchport access vlan 102
!
interface VLAN 101
 ipv6 address 1010::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 102
 ipv6 address 1020::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 103
 ipv6 address 1030::1/64
 ipv6 ospf 4949 area 0
!
interface VLAN 104
 ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
!
ipv6 router ospf 4949
 graceful-restart
!
ipv6 mld snooping svgl vlan 104
ipv6 mld snooping svgl profile 1
ipv6 mld snooping ivgl-svgl
!
```

- Device C configuration file

```
hostname DeviceC
!
ipv6 multicast-routing
!
interface GigabitEthernet 0/21
 no switchport
 ipv6 address 1000::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet 0/23
 no switchport
 ipv6 address 1010::3/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
ipv6 router ospf 4949
 graceful-restart
!
```

7. Common Errors

- The multicast groups associated with the SVGL mode are not configured.
- The address of sent multicast traffic is not within the range of multicast groups associated with the SVGL mode.
- The multicast group addresses of multicast traffic in IVGL mode are within the multicast group range in SVGL mode. As a result, IVGL forwarding cannot be implemented.

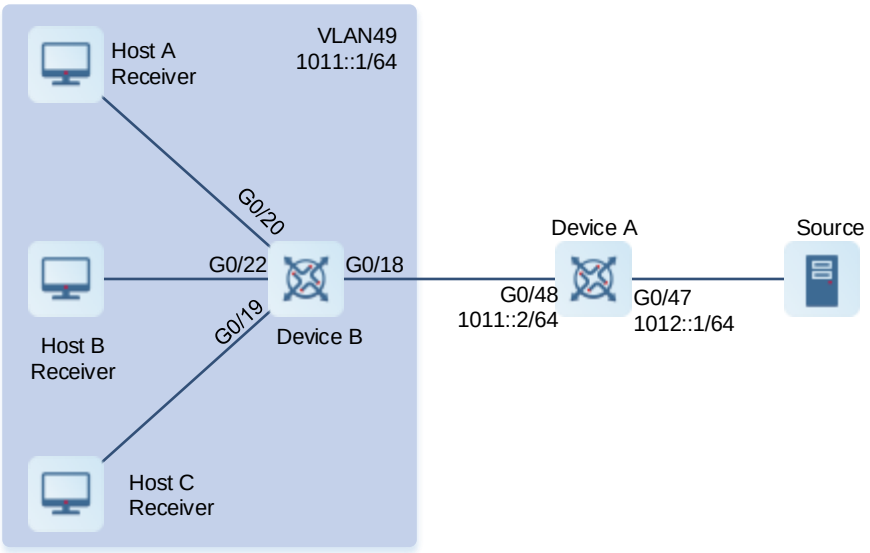
1.7.4 Configuring Static Ports to Implement L2 Multicast

1. Requirements

In the multicast network shown in Figure 1-8, Host A, Host B, and Host C need to receive data that a multicast source sends to a specific multicast group stably. The router (Device A) connects to the user network through the L2 device (Device B). The static MLD multicast groups FF14::10 to FF14::12 are configured on the user-side L3 port on Device A. Host A and Host B want to receive data of multicast group FF14::10 stably, and Host C wants to receive data of multicast group FF14::11.

2. Topology

Figure 1-8 Topology of Static Ports to Implement L2 Multicast



3. Notes

Configure MLD snooping static multicast router ports and member ports on Device B.

- Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.
- Enable multicast routing and MLD static multicast groups on Device A.
- Enable MLD snooping on Device B.
- Configure static multicast router ports and member ports on Device B.

4. Procedure

(1) Configure the IPv6 addresses, VLANs, and unicast routing protocols of the network nodes to ensure reachability of the network nodes using unicast routing.

Configure the IPv6 address and unicast routing protocol on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 0/47
DeviceA(config-if-GigabitEthernet 0/47)# no switchport
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 address 1012::1/64
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# no switchport
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 address 1011::2/64
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 ospf 4949 area 0
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ipv6 router ospf 4949
DeviceA(config-router)# exit
```

Configure the IPv6 address, VLAN, and unicast routing protocol on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan 49
DeviceB(config-vlan)# exit
DeviceB(config)# interface vlan 49
DeviceB(config-if-VLAN 49)# ipv6 address 1011::1/64
DeviceB(config-if-VLAN 49)# ipv6 ospf 4949 area 0
DeviceB(config-if-VLAN 49)# exit
DeviceB(config)# interface GigabitEthernet 0/18
DeviceB(config-if-GigabitEthernet 0/18)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/18)# exit
DeviceB(config)# interface GigabitEthernet 0/19
DeviceB(config-if-GigabitEthernet 0/19)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/19)# exit
DeviceB(config)# interface GigabitEthernet 0/20
DeviceB(config-if-GigabitEthernet 0/20)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/20)# exit
DeviceB(config)# interface GigabitEthernet 0/22
DeviceB(config-if-GigabitEthernet 0/22)# switchport access vlan 49
DeviceB(config-if-GigabitEthernet 0/22)# exit
DeviceB(config)# ipv6 router ospf 4949
DeviceB(config-router)# exit
```

(2) Enable IPv6 multicast routing and PIM-SMv6 related functions on Device A.

```
DeviceA(config)# ipv6 multicast-routing
DeviceA(config)# interface GigabitEthernet 0/47
```

```
DeviceA(config-if-GigabitEthernet 0/47)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/47)# exit
DeviceA(config)# interface GigabitEthernet 0/48
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 mld static-group ff14::10
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 mld static-group ff14::11
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 mld static-group ff14::12
DeviceA(config-if-GigabitEthernet 0/48)# ipv6 pim sparse-mode
DeviceA(config-if-GigabitEthernet 0/48)# exit
DeviceA(config)# ipv6 pim bsr-candidate GigabitEthernet 0/47
DeviceA(config)# ipv6 pim rp-candidate GigabitEthernet 0/47
```

(3) Enable MLD snooping functions on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld snooping ivgl
```

(4) Configure static multicast router ports and member ports on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 mld snooping vlan 49 static ff14::11 interface
GigabitEthernet 0/19
DeviceB(config)# ipv6 mld snooping vlan 49 static ff14::10 interface
GigabitEthernet 0/22
DeviceB(config)# ipv6 mld snooping vlan 49 static ff14::10 interface
GigabitEthernet 0/20
DeviceB(config)# ipv6 mld snooping vlan 49 mrouter interface GigabitEthernet 0/18
```

5. Verification

Run the **show ipv6 mld snooping mrouter** command and check whether the static router port is GigabitEthernet 0/18.

```
DeviceB> enable
DeviceB# show ipv6 mld snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 49):
  VLAN(49)  1 MROUTES:
    GigabitEthernet 0/18(DS)

(*, *, 101):
  VLAN(101)  1 MROUTES:
    GigabitEthernet 0/21(D)

DeviceB#
```

Run the **show ipv6 mld snooping gda-table** command and check whether the static member ports of multicast group FF14::10 are GigabitEthernet 0/20 and GigabitEthernet 0/22 and the static member port of multicast group FF14::11 is GigabitEthernet 0/19.

```
DeviceB# show ipv6 mld snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, FF14::10, 49):
  VLAN(49) 3 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/20(S)
    GigabitEthernet 0/22(S)

(*, FF14::11, 49):
  VLAN(49) 2 OPORTS:
    GigabitEthernet 0/18(M)
    GigabitEthernet 0/19(S)

DeviceB#
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ipv6 multicast-routing
!
interface GigabitEthernet0/47
 no switchport
 ipv6 address 1012::1/64
 ipv6 ospf 4949 area 0
 ipv6 pim sparse-mode
!
interface GigabitEthernet0/48
 no switchport
 ipv6 address 1011::2/64
 ipv6 ospf 4949 area 0
 ipv6 mld static-group ff14::10
 ipv6 mld static-group ff14::11
 ipv6 mld static-group ff14::12
 ipv6 pim sparse-mode
!
Ipv6 router ospf 4949
 graceful-restart
!
ipv6 pim bsr-candidate GigabitEthernet 0/47
ipv6 pim rp-candidate GigabitEthernet 0/47
!
```

- Device B configuration file

```
hostname DeviceB
!
vlan range 1,49
!
interface GigabitEthernet 0/18
 switchport access vlan 49
!
interface GigabitEthernet 0/19
 switchport access vlan 49
!
interface GigabitEthernet 0/20
 switchport access vlan 49
!
interface GigabitEthernet 0/22
 switchport access vlan 49
!
interface VLAN 49
 ipv6 address 1011::1/64
 ipv6 ospf 4949 area 0
!
router ospf 49
 graceful-restart
!
ipv6 mld snooping ivgl
!
ipv6 mld snooping vlan 49 static FF14::11 interface GigabitEthernet 0/19
ipv6 mld snooping vlan 49 static FF14::10 interface GigabitEthernet 0/22
ipv6 mld snooping vlan 49 static FF14::10 interface GigabitEthernet 0/20
ipv6 mld snooping vlan 49 mrouter interface GigabitEthernet 0/18
!
```

7. Common Errors

- Basic MLD snooping functions are not configured or fail to be configured.

ACL and QoS Configuration

1. ACL Configuration
2. QoS Configuration
3. MMU Configuration

Contents

1 Configuring ACL 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Configuration Task Summary 14
1.3 Configuring an IP Standard ACL 14
1.3.1 Overview 14
1.3.2 Restrictions and Guidelines 14
1.3.3 Configuration Tasks 14
1.3.4 Creating an IP Standard ACL 15
1.3.5 Applying an IP Standard ACL 16
1.3.6 Configuring a Global Security ACL 17
1.3.7 Configuring a Security Channel 18
1.3.8 Configuring a Redirect ACL 19
1.3.9 Configuring the Fragmented Packet Matching Mode 20
1.3.10 Configuring the SVI Router ACL 20
1.4 Configuring an IP Extended ACL 21
1.4.1 Overview 21
1.4.2 Restrictions and Guidelines 21
1.4.3 Configuration Tasks 21
1.4.4 Creating an IP Extended ACL 21
1.4.5 Applying an IP Extended ACL 23
1.4.6 Configuring a Global Security ACL 24

1.4.7 Configuring a Security Channel 25

1.4.8 Configuring a Redirect ACL 26

1.4.9 Configuring the Fragmented Packet Matching Mode 26

1.4.10 Configuring the SVI Router ACL 27

1.5 Configuring a MAC Extended ACL 27

1.5.1 Overview 27

1.5.2 Restrictions and Guidelines 27

1.5.3 Configuration Tasks 28

1.5.4 Creating a MAC Extended ACL 28

1.5.5 Applying a MAC Extended ACL 29

1.5.6 Configuring a Security Channel 30

1.5.7 Configuring a Redirect ACL 31

1.5.8 Configuring the SVI Router ACL 32

1.6 Configuring an Expert Extended ACL 32

1.6.1 Overview 32

1.6.2 Restrictions and Guidelines 32

1.6.3 Configuration Tasks 32

1.6.4 Creating an Expert Extended ACL 33

1.6.5 Applying an Expert Extended ACL 34

1.6.6 Configuring a Global Security ACL 35

1.6.7 Configuring a Security Channel 36

1.6.8 Configuring a Redirect ACL 37

1.6.9 Configuring the Fragmented Packet Matching Mode 37

1.6.10 Configuring the SVI Router ACL 38

1.7 Configuring an IPv6 ACL 38
1.7.1 Overview 38
1.7.2 Restrictions and Guidelines 38
1.7.3 Configuration Tasks 38
1.7.4 Creating an IPv6 ACL 39
1.7.5 Applying an IPv6 ACL 40
1.7.6 Configuring a Global Security ACL 41
1.7.7 Configuring a Security Channel 42
1.7.8 Configuring a Redirect ACL 43
1.7.9 Configuring the SVI Router ACL 44
1.8 Configuring an Expert Advanced ACL (ACL80) 44
1.8.1 Overview 44
1.8.2 Restrictions and Guidelines 44
1.8.3 Configuration Tasks 44
1.8.4 Creating an ACL80 44
1.8.5 Applying an ACL80 45
1.8.6 Configuring the SVI Router ACL 46
1.9 Monitoring 46
1.10 Examples 48
1.10.1 Configuring an IP Standard ACL 48
1.10.2 Configuring an IP Extended ACL 49
1.10.3 Configuring a MAC Extended ACL 54
1.10.4 Configuring an Expert Extended ACL 56
1.10.5 Configuring an IPv6 ACL 59

1.10.6 Configuring an ACL80 60

1.10.7 Configuring a Global Security ACL 63

1.10.8 Configuring ACL Rules Based on Time Range 65

1 Configuring ACL

1.1 Introduction

1.1.1 Overview

The access control list (ACL) is also called access list or packet filtering in some documents. An ACL defines a series of "permit" or "deny" rule statements, and applies these rules to a device interface to control the data packets entering/leaving the interface, so as to improve the security of network devices.

Configuring ACL can guarantee network security, reliability, and stability, for example:

- Preventing packet attacks: An ACL can be configured to deny the attacks launched using the Internet Protocol (IP), Transmission Control Protocol (TCP), or Internet Control Message Protocol (ICMP) packets.
- Controlling network access: An ACL can be configured to restrict users to some services, for example, users are allowed to access only the WWW and email services, but not allowed to access other services such as telnet; some users are allowed to access services only within a given time period, or only certain hosts are allowed to access the network.
- Controlling network traffic: An ACL can be used together with quality of service (QoS) to guarantee prioritized services for some important data flows. For QoS configuration, see "Configuring QoS."

1.1.2 Principles

1. Basic Concepts

- ACL

ACLs are classified into basic ACLs and dynamic ACLs.

Users can select a basic ACL or a dynamic ACL as needed. In general, a basic ACL can meet security requirements. However, experienced hackers may counterfeit source addresses by using some software to spoof devices and access the network. Before users access the network, the dynamic ACL requires them to pass identity authentication, which makes it hard for hackers to attack the network. Therefore, the dynamic ACL can be used in some sensitive areas to ensure network security.

Note

Spoofing devices by counterfeiting source addresses, namely, spoofing, is an inherent problem of all ACLs. Spoofing also occur on the dynamic ACL: Hackers may fake users' addresses to access the network during the effective access period after the users pass the identity authentication. This problem can be solved in two ways. One is to set the idle time of user access to a smaller value so that it is more difficult for hackers to break into the network. The other is to use the IP Security (IPSec) encryption protocol to encrypt the network data, and ensure that all the data is encrypted when the data is transmitted to a device.

The ACL is generally configured on the following network devices:

- A device between an internal network and an external network (such as the Internet)
- A device at the boundary of two parts of the network

- A device connecting to a control port

- ACE

  An access control entry (ACE) is a statement containing the "permit" or "deny" action and filtering rules. Each ACE has a sequence number, which is automatically allocated by the device or manually configured. An ACL contains one or more ACEs. The ACL identifies and filters packets by using ACEs.

  The sequence of ACEs in an ACL determines the matching priority of the ACEs in the ACL. When processing packets, a network device performs rule matching in the ascending order of ACE sequence numbers. When finding a matched ACE, the network device stops matching subsequent ACEs.

  For example, create ACE 10 to deny all data flows.

```
10 deny ip any any
20 permit tcp 192.168.12.0 0.0.0.255 eq telnet any
```

  Since ACE 10 denies all the IP packets, the telnet packet from the host in the 192.168.12.0/24 network is denied even if it matches ACE 20. The reason is that, after finding that the packet matches the first ACE, the device stops matching the packet with the subsequent ACE 20.

  Here is another example: Create ACE 10 to permit all IPv6 data flows to pass through.

```
10 permit ipv6 any any
20 deny ipv6 host 200::1 any
```

  Since ACE 10 permits all IPv6 packets to pass through, the IPv6 packet sent from the host with IP address 200::1 can pass through even if it matches ACE 20. The reason is that, after finding that the packet matches the first ACE, the device stops matching the packet with the subsequent ACE 20.

- Step

  When the device automatically allocates sequence numbers to ACEs, the difference between two adjacent ACE sequence numbers is called a step. For example, if the step is set to 5, the device automatically allocates sequence numbers to ACEs in the ascending order of 5, 10, 15.... See the example below.

```
5 deny ip any any
10 permit tcp 192.168.12.0 0.0.0.255 eq telnet any
```

  After the step is changed, the ACE sequence numbers will be automatically rearranged based on the new step value. For example, when the step is changed to 10, the original ACE sequence numbers are changed from 5, 10, and 15 to 5, 15, and 25.

  A new ACE can be inserted between two ACEs by changing the step. For example, four ACEs are created, and the ACEs are manually numbered 1, 2, 3, and 4 in turn. To insert a new ACE after ACE 1, first change the step to 2 (then, the sequence numbers of the original four ACEs automatically change to 1, 3, 5, and 7), and then insert a manually configured ACE with sequence number 2.

- Filter field template

  Filter fields mean the fields used to identify and classify packets when an ACE is generated. A filter field template is a combination of such fields. An ACE identifies Ethernet packets by some fields in them, including:

  L2 fields:

  - 48-bit source MAC address (the 48-bit source MAC address must be matched completely)
  - 48-bit destination MAC address (the 48-bit destination MAC address must be matched completely)

- 16-bit L2 type field

L3 fields:

- Source IP address field (all the source IP address values can be matched or a subnet can be used to define a type of flow)
- Destination IP address field (all the destination IP address values can be matched or a subnet can be used to define a type of flow)
- Protocol type field

L4 fields:

- You can define a TCP source port, destination port, or both for matching; you can also define the range of the source port or destination port for matching.
- You can define a User Datagram Protocol (UDP) source port, destination port, or both for matching; you can also define the range of the source port or destination port for matching.

For example, you can create an ACE to identify and classify packets based on their destination IP address field. You can also create another ACE to identify and classify packets based on their source IP address field and UDP source port field. These two ACEs use different filter field templates.

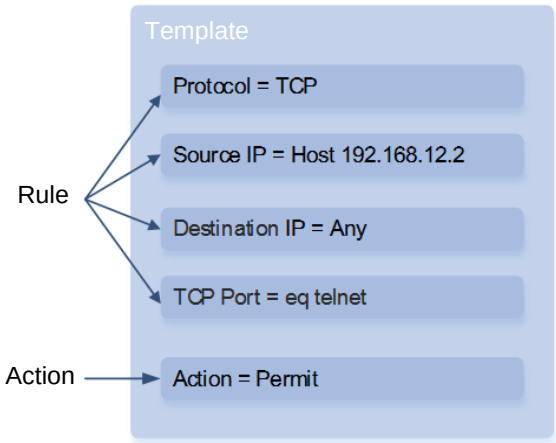
- Rules

Rules refer to the values of fields in an ACE filter field template. For example, an ACE reads as follows:

```
10 permit tcp host 192.168.12.2 any eq telnet
```

In this ACE, the filter field template is a collection of the following fields: source IP address field, destination IP address field, IP protocol field, and TCP destination port field. The corresponding values (namely, rules) are as follows: The source IP address is **Host 192.168.12.2**, the destination IP address is **Any** (namely, all the hosts), the IP protocol is **TCP**, and the TCP destination port is **Telnet**. See Figure 1-1.

Figure 1-1 Analysis of ACE: permit tcp host 192.168.12.2 any eq telnet



Note

- A filter field template can be a collection of L3 fields and L4 fields, or a collection of multiple L2 fields. However, the filter field templates of the standard and extended ACLs cannot be a collection of L2 and L3 fields, or L2 and L4 fields, or L2, L3, and L4 fields. To use a collection of L2, L3, and L4 fields, you can use an expert extended ACL.

- Outbound ACLs to be associated with switch virtual interfaces (SVIs) can be IP standard, IP extended, MAC extended, or expert ACLs.
- If a destination MAC address is configured for matching in MAC extended and expert ACLs and such ACLs are applied in the outbound direction of an SVI, the ACEs containing the destination MAC address can be configured but fail to take effect. If you configure a destination IP address for matching in the IP extended and expert ACLs but the destination IP address is not within the subnet IP address range of the associated SVI, the configured ACLs do not take effect. For example, if VLAN 1 has an IP address 192.168.64.1 255.255.255.0 and an IP extended ACL is created, with the ACE **deny udp any 192.168.65.1 0.0.0.255 eq 255**, this ACL does not take effect when it is applied to the egress of VLAN 1. The cause is that the destination IP address is not within the subnet IP address range of VLAN 1. If the ACE is **deny udp any 192.168.64.1 0.0.0.255 eq 255**, the ACL takes effect because the destination IP address complies with the requirements.

Note

- When an expert ACL is configured and applied to the outbound direction of a port, if some ACEs in the ACL contain L3 matching information (such as IP address and L4 port), the non-IP packets received by the port cannot be subjected to the permit and deny ACEs of the ACL.

2. IP ACL

IP ACL implements refined control over the IPv4 packets entering/leaving the device. You can deny or permit specific IPv4 packets destined to a network according to the actual needs, so as to control the access of IP users to network resources.

You can define a series of access rules in an IP ACL, and apply the ACL to the inbound or outbound direction of a port. You can also apply an IP ACL globally. When IPv4 packets enter or leave a device, the device determines whether to forward or block them by judging whether they match the rules.

To configure an IP ACL on a device, you must specify a unique name or number for each ACL to uniquely identify the ACL.

IP ACLs are classified into IP standard ACLs and IP extended ACLs. Table 1-1 lists the ranges of numbers that can be used for IP standard ACLs and IP extended ACLs.

Table 1-1 Number Ranges for IP Standard ACLs and IP Extended ACLs

Type	Number Range	Matching Field
IP standard ACL	1 to 99, 1300 to 1999	Source IP address
IP extended ACL	100 to 199, 2000 to 2699	• Source IP address • Destination IP address • IP protocol number • L4 source port ID or ICMP type • L4 destination port ID or ICMP code

The IP standard ACL controls the forwarding or blocking of packets based on the source IP address. The IP extended ACL controls the forwarding or blocking of packets by combining the matching fields in the table above.

A single ACL can use multiple independent ACL statements to define multiple rules, and all the statements use the same number or name so that the statements are bound to the same ACL.

Note

On routers, the ICMP code matching field in ACL rules is invalid for the ICMP packets with ICMP type 3. If the code field for matching ICMP packets is configured in an ACL rule, when ACL matching is performed on the ICMP packets with type 3 on the routers, the matching result may be different from the expected result.

One rule statement of denying all data flows is hidden at the end of each IP ACL. If a packet fails to match any rules, it will be denied. For example:

```
access-list 1 permit host 192.168.4.12
```

This ACL only permits the packets with source host address 192.168.4.12 to pass through, and denies the packets of the other hosts. The reason is that this ACL contains a rule statement at its end as follows:

```
access-list 1 deny any
```

Here is another example:

```
access-list 1 deny host 192.168.4.12
```

If an ACL contains the above statement only, the packets of all the hosts are denied wen passing through the port.

Warning

When defining an ACL, you must consider the route update packets. The rule statement of denying all data flows at the end of the ACL may result in blocking of all the route update packets.

The reflexive ACL automatically generates a temporary ACL according to the L3 and L4 information of the traffic originated from the internal network. A temporary ACL is created according to the following principles: The IP protocol number remains unchanged, the source IP address and destination IP address are strictly interchanged, and the TCP/UDP source port and destination port are strictly interchanged. Only when the L3 and L4 information of the returned traffic strictly matches that in the temporary ACL previously created based on the outbound traffic, will the device permit the traffic to enter the internal network.

3. MAC Extended ACL

The MAC extended ACL implements refined control over the packets entering/leaving the device based on the L2 information of the packets. You can deny or permit specific L2 packets destined to a network according to the actual needs, so as to protect network resources against attacks or control the access of users to network resources.

You can define a series of access rules in a MAC extended ACL, and apply the ACL to the inbound or outbound direction of a port. When packets enter or leave a device, the device determines whether to forward or block them by judging whether they match the rules.

To configure a MAC extended ACL on a device, you must specify a unique name or number for each ACL to uniquely identify the ACL. Table 1-2 lists the range of numbers for the MAC extended ACLs.

Table 1-2 Number Range for MAC Extended ACLs

Type	Number Range	Matching Field
MAC extended ACL	700 to 799	● Source MAC address ● Destination MAC address ● Ethernet protocol type

The MAC extended ACL controls the forwarding or blocking of packets based on the source or destination MAC address and the Ethernet type of packets.

A single MAC extended ACL can use multiple independent ACL statements to define multiple rules, and all the statements use the same number or name so that the statements are bound to the same ACL.

Note

If a MAC extended ACL rule does not specify IPv6 packets, that is, the Ethernet type field is not defined or the defined Ethernet type field value is not 0x86dd, then the MAC extended ACL is not used to match IPv6 packets. If you need to match IPv6 packets, define an IPv6 ACL.

One rule statement of denying all data flows is hidden at the end of each MAC extended ACL. If a packet fails to match any rules, it will be denied. For example:

```
access-list 700 permit host 00d0.f800.0001 any
```

This ACL permits only the packets sent from the host with MAC address 00d0.f800.0001 to pass through, and denies the packets from all the other hosts. The reason is that this ACL contains a rule statement at its end as follows:

```
access-list 700 deny any any
```

4. Expert Extended ACL

The expert extended ACL is also known as expert-level extended ACL. The expert extended ACL implements refined control over the packets entering/leaving a device based on the L2 and L3 information of the packets. The expert extended ACL can be regarded as a combination and enhancement of the IP ACL and MAC extended ACL. An expert extended ACL can contain IP ACL rules and MAC extended ACL rules, and specify VLAN IDs for packet matching.

You can define a series of access rules in an expert extended ACL, and apply the ACL to the inbound or outbound direction of a port. When packets enter or leave a device, the device determines whether to forward or block them by judging whether they match the access rules.

To configure an expert extended ACL on a device, you must specify a unique name or number for each ACL to uniquely identify the ACL. Table 1-3 lists the range of numbers that can be used for expert extended ACLs.

Table 1-3 Number Range for Expert Extended ACLs

Type	Number Range	Matching Field
Expert extended ACL	2700 to 2899	● Source IP address ● Destination IP address ● IP protocol number ● L4 source port ID or ICMP type ● L4 destination port ID or ICMP code ● Source MAC address ● Destination MAC address ● Ethernet protocol type ● VLAN ID

The expert extended ACL controls the forwarding or blocking of packets by combining the matching fields in the table above.

A single expert extended ACL can use multiple independent ACL statements to define multiple rules, and all the statements must use the same number or name so that the statements are bound to the same ACL.

One rule statement of denying all data flows is hidden at the end of each expert extended ACL. If a packet fails to match any rules, it will be denied. For example:

```
access-list 2700 permit 0x0806 any any any any any
```

This ACL only permits the packets with Ethernet type 0x0806 (namely, ARP) to pass through, and denies the packets of the other types. The reason is that this ACL contains a rule statement at its end as follows:

```
access-list 2700 deny any any any any
```

5. IPv6 ACL

The IPv6 ACL implements refined control over the IPv6 packets entering/leaving a device. You can deny or permit specific IPv6 packets destined to a network according to the actual needs, so as to control the access of IPv6 users to network resources.

You can define a series of access rules in an IPv6 ACL, and apply the ACL to the inbound or outbound direction of a port. When IPv6 packets enter or leave a device, the device determines whether to forward or block them by judging whether they match the rules.

To configure an ACL on a device, you must specify a unique name for the ACL of a protocol.

Note

- Different from IP ACLs, MAC extended ACLs, and expert extended ACLs, an IPv6 ACL must have the name rather than the number specified during creation.
- Only one IP ACL, one MAC extended ACL, or one expert extended ACL can be applied to the inbound or outbound direction of a device port. Besides, an IPv6 ACL can be applied.

One rule statement of denying all IPv6 data flows is hidden at the end of each IPv6 ACL. If a packet fails to match any rules, it is denied. For example:

```
ipv6 access-list ipv6_acl
 10 permit ipv6 host 200::1 any
```

This ACL only permits the IPv6 packets coming from source host 200::1 to pass through, and denies the IPv6 packets from all the other hosts. The reason is that this ACL contains a rule statement at its end as follows:

```
deny ipv6 any any
```

Warning

Although each IPv6 ACL contains the rule statement of denying all the IPv6 packets by default, it does not deny neighbor discovery (ND) packets.

6. ACL80

ACL80 is the expert advanced ACL, also known as user-defined ACL. ACL80 supports matching the specified bytes in the first 80 bytes of a packet by bit.

There are three elements in ACL80 matching: matching field content, matching field mask, and the start position (that is, the offset) of matching. The bits of the matching field content map to those of the matching field mask. The matching field content specifies the field value to be matched, and the matching field mask specifies whether the corresponding bits need to be matched. When a bit needs to be matched, the corresponding bit in the matching field mask must be set to **1**. If a bit in a matching field mask is set to **0**, the corresponding bit in the matching field content will not be matched regardless of the bit value in the matching field content. For example:

```
10 permit 00d0f8123456 ffffffffffff 0
20 deny 00d0f8654321 ffffffffffff 6
```

In ACE 10, the matching field content is 00d0f8123456, the matching field mask is ffffffffffff, and the offset is 0. This rule indicates that, if the destination MAC address of a packet is 00d0f8123456, the packet is permitted to be forwarded.

In ACE 20, the matching field content is 00d0f8654321, the matching field mask is ffffffffffff, and the offset is 6. This rule indicates that, if the source MAC address of a packet is 00d0f8654321, the packet is blocked.

You need to deeply understand the L2 data frame structure so as to use the user-defined ACL correctly. Figure 1-2 shows the first 64 bytes of an L2 data frame. In the figure, each letter represents one hexadecimal number and every two letters represent one byte.

Figure 1-2 First 64 Bytes of an L2 Data Frame

AA	AA	AA	AA	AA	AA	BB	BB	BB	BB	BB	BB	CC	CC	DD	DD
DD	DD	EE	FF	GG	HH	HH	HH	II	II	JJ	KK	LL	LL	MM	MM
NN	NN	OO	PP	QQ	QQ	RR	RR	RR	RR	SS	SS	SS	SS	TT	TT
UU	UU	VV	VV	VV	VV	ww	ww	ww	ww	XY	ZZ	aa	aa	bb	bb

Table 1-4 lists the meaning and offset value of each letter.

Table 1-4 Meanings and Offset Values of Letters

Letter	Description	Offset	Letter	Description	Offset
A	Destination MAC address	0	O	TTL field	34
B	Source MAC address	6	P	Protocol number	35
C	VLAN tag field	12	Q	IP checksum	36
D	Data frame length field	16	R	Source IP address	38
E	Destination service access point (DSAP) field	18	S	Destination IP address	42
F	Source service access point (SSAP) field	19	T	TCP source port	46
G	Control field	20	U	TCP destination port	48
H	Org code field	21	V	Serial number	50
I	Encapsulated data type	24	W	Acknowledgment field	54
J	IP version No.	26	XY	IP header length and reserved bits	58
K	ToS field	27	Z	Reserved bits and flags bits	59
L	IP packet length	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

The offset of each field in the table is their offset in the IEEE 802.3 data frame containing the SNAP+Tag fields. The user-defined ACL extracts specific fields from the first 80 bytes of a data frame according to offsets listed in Table 1-5, and then compare the fields with the matching field masks so as to determine the matching field content. For example, if you permit all TCP packets to be forwarded, you can set the matching field content to **06**, the matching field mask to **ff**, and the offset to **35**. Create ACE 10 as follows:

```
10 permit 06 ff 35
```

Apply the ACL to the inbound or outbound direction of a port. When a packet enters or leaves a device, ACL80 extracts the content of the TCP protocol number field from the data frame, and then compares the content with the matching field content to find out all the matched TCP packets for forwarding.

Note

- ACL80 supports matching Ethernet packets, IEEE 802.3 SNAP packets, and IEEE 802.3 LLC packets. If the values of the **DSAP** field to the **Control** field to be matched are **AAAA03**, the IEEE 802.3 SNAP packets need to be matched. If the values of the **DSAP** field to the **Control** field to be matched are **E0E003**, the 802.3 LLC packets need to be matched. You cannot set the matching of these fields for Ethernet packets.

- Due to hardware reasons, currently ACL80 cannot implement random byte matching for the first 80 bytes of packets, but only supports matching the locations of the destination MAC address, source MAC address, VLAN ID, ETYPE, IP protocol number, source IPv4 address, destination IPv4 address, source port, destination port, ICMP_TYPE, ICMP_CODE, and PPPOE_IPTYPE fields in packets.
- When an ACL80 is used to match IP, ARP, and other information, the encapsulated data type and data type mask need to be configured first, that is, the field with offset 24 needs to be configured first, and the mask needs to be set to all Fs. For example, to allow the packets with the source IP address 192.168.1.2 to pass through, the corresponding configuration command is **permit 0800 FFFF 24 C0A80102 FFFFFFFF 38**.

7. Redirect ACL

Redirect ACL enables a device to analyze a received packet and redirect it to a specified port for forwarding. To analyze specific packets entering the device, you can configure the redirect ACL function to redirect the packets conforming to the rules to a specified port, which captures the packets for analysis.

Redirect ACL binds an ACL on an input port and specifies an output port. When the input port receives a packet, it queries ACL rules bound to the port one by one. If the packet conforms to the characteristics described in a rule, it is forwarded from the output port specified by the policy.

Note

- Redirect ACL takes effect only in the inbound direction of a port
- Only one global redirect ACL can be configured.
- When the global redirect ACL is configured with the destination port, the port is not affected by the global redirect ACL.

8. Global Security ACL

There are various virus packets in the network, and the identification characteristics of virus packets are the same or similar on each port. You can create an ACL, add ACEs that match the characteristics of various virus packets, and apply the ACL to each port of a device to filter out virus packets. Such an ACL is called port-based security ACL. In consideration of secure deployment, a port-based security ACL is often configured to filter out packets that comply with some characteristics (such as forged TCP attack packets) and prevent virus packets.

When the port-based security ACL is used in the attack-defense scenarios such as virus filtering, there are much inconvenience.

- Ports must be configured one by one. Duplicate configuration, poor operating performance, and excessive consumption of ACL resources can occur.
- The access control function of the security ACL is weakened. Because the security ACL is used for virus filtering, the basic functions of the security ACL including restricting route updates and restricting network access become unavailable.

The global security ACL can be used for global anti-virus deployment and defense without affecting the port-based security ACL. A global security ACL can take effect on all the L2 ports after one command is configured.

When both the global security ACL and port-based security ACL are configured, they take effect at the same time. The packets that match rules in the global security ACL will be directly filtered out as virus packets, and the packets that fail to match the rules of the global security ACL are still controlled by the port-based security ACL. To exempt some ports from the control of the global security ACL, disable the global security ACL function on

these ports. When the global, port-based, and VLAN-based security ACLs are applied at the same time, the priority is port-based security ACL, VLAN-based security ACL, and global security ACL in the descending order.

To avoid misconfiguration of the global security ACL, the global security ACL disabling function is provided. If you disable the global security ACL function and then configure a global security ACL, the system prompts a configuration failure. If you have configured a global security ACL and then disable the global security ACL function, the system deletes all the current global security ACLs and displays a log prompt.

Note

- Since the global security ACL is mainly used for virus filtering, among the ACEs in a global security ACL, only the deny ACEs are installed and take effect, and the permit ACEs will not take effect.
- Different from a security ACL applied to a port, a global security ACL has no default rule statement of denying all data flows, that is, packets not matching the rules in a global security ACL can pass through.
- A global security ACL can take effect on both L2 ports and L3 ports. That is, it can take effect on the following types of ports: access port, trunk port, hybrid port, L3 Ethernet port, L2 or L3 aggregation port. It does not take effect on SVIs.
- You can disable the global security ACL independently on physical ports and L2 or L3 aggregation ports, but not on the member ports of an aggregation port.
- Global security ACLs can be associated only with IP standard ACLs, IP extended ACLs, MAC extended ACLs, and expert extended ACLs.

9. Security Channel

In some application scenarios, the packets complying with certain characteristics must bypass the check of access control application. For example, before the IEEE 802.1x authentication, users must be allowed to log in to the specified resource site and download the IEEE 802.1x authentication client.

This can be achieved through the security channel. A security channel is also an ACL, which can be configured globally or on ports. Applying a security ACL globally or to a port by using a security channel configuration command means that the ACL is a security channel.

When entering a device port, a packet is first checked by the security channel. If the packet meets the matching conditions of the security channel, it bypasses the access control such as port security, Web authentication, IEEE 802.1x, and IP + MAC binding check, and directly enters the device. The security channel applied globally takes effect for all the non-excluded ports.

Note

- The deny behavior in an ACL applied as a security channel does not take effect, and there is no rule statement of denying all data flows hidden at the end. If a packet does not meet the matching conditions of a security channel, it goes through the check of access control according to the process.
- You can set up to eight excluded ports for the global security channel, and no port-based security channel can be configured on the excluded ports of the global security channel.
- When both the port-based authentication migration mode and security channel are used, the security channel does not take effect.
- You cannot configure an IPv6 ACL as a security channel.

10. SVI Router ACL

An ACL applied to an SVI (namely, SVI ACL) takes effect for both the packets forwarded on L2 in a VLAN and the inter-VLAN routed packets. As a result, different users in the same VLAN cannot make normal communication. The SVI router ACL function enables the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

The SVI router ACL function is disabled by default. The SVI ACL takes effect for the inter-VLAN L3 forwarded packets and the intra-VLAN packets forwarded by bridges. After the SVI router ACL function is enabled, the SVI ACL is effective only for the inter-VLAN L3 forwarded packets.

11. Packet Matching Logging

The packet matching logging is used to monitor the running status of ACL rules and provide necessary information for routine network maintenance and network optimization.

To better grasp the running status of ACL in the device, when adding ACEs, you can decide whether to specify the packet matching logging option as needed. If this option is specified, the matching logs are output when ACEs match packets. ACL prints log information based on ACE, that is, the device periodically prints the ACEs that match packets and the number of matched packets. See the example below:

```
*Sep  9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78
packets.
```

To reasonably control the quantity and frequency of log output, ACL allows configuring the log output interval.

Warning

An ACL rule with the log option uses more hardware resources. If all the configured rules have the log option, the hardware policy capacity of the device is halved.

Caution

- The default output interval of packet matching logs is 0 minutes, that is, no ACL matching log is output. After specifying the log option when configuring ACL rules, you also need to configure the output interval, otherwise no matching log is output.
- For a rule with the log option, if no packet matches the rule within the specified time interval, no packet matching log related to the rule is output; if a packet matches the rule within the specified time interval, the packet matching log related to the rule is output after the time interval expires. The number of matched packets is the total number of packets matching the rule within the time interval, that is, the number of matched packets from the last log output to the current log output.

12. Packet Matching Counting

For the needs of network management, you may want to know whether an ACL rule matches packets and the number of matched packets. ACL provides the rule-based packet matching counting function. You can enable or disable the packet matching counting function for all the rules in an ACL. When a packet matches a rule, the corresponding matching count increases accordingly. You can run the statistics clearing command for an ACL to clear the packet matching counts of all rules in the ACL and start new counting.

Warning

Enabling the packet matching counting function of ACL requires more hardware entries, and in extreme cases, halves the available hardware policy capacity of the device.

13. ACL Effective Time Range

If you need to control some flows within a specified time range, for example, disable chat tools during working hours, you can configure effective time ranges for ACEs to control the pass-through time of flows. The time ranges are classified into absolute time ranges and periodic time ranges.

An absolute time range indicates the time range from the specified start time to the end time. This time range does not occur cyclically nor has a period, for example, "12:00:00 on January 1, 2000 to 12:00:00 on January 1, 2001".

A periodic time range indicates a periodic time interval, for example, "8:00 on each Monday to 17:00 on each Friday".

For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".

14. Fragmented Packet Matching Mode

The fragmented packet matching mode enables ACL to control fragmented packets more finely.

IP packets may be fragmented during network transmission. When a packet is fragmented, only the first fragment carries L4 information, such as the TCP or UDP port ID, ICMP type, and ICMP code. Other fragmented packets do not carry the L4 information. By default, if an ACL rule carries the fragment flag, only the non-first fragments are matched; if an ACL rule does not carry the fragment flag, all the packets, including the first fragment and all the subsequent fragmented packets, are matched. In addition to the default fragmented packet matching mode, another new fragmented packet matching method is provided. You can switch between the modes on a specified ACL as needed. In the new fragmented packet matching mode, when an ACL rule does not carry the **fragment** option, if a packet is fragmented, the first fragment will be matched with all the user-defined matching fields in the rule (including the L3 and L4 information) and non-first fragments will be matched only with non-L4 information in the rule.

Warning

- In the new fragmented packet matching mode, if an ACL rule does not carry the fragment flag and the matching action is permit, such an ACL rule needs to occupy more hardware entry resources, and, in extreme cases, halves the capacity of hardware policy entries. If such an ACE is configured with **Established** in TCP flag filter control, more hardware policy entry resources will be occupied.
- When you switch the fragmented packet matching mode, the ACL fails for a short period of time.

15. Global Control Plane Security ACL

In some application scenarios, an ACL needs to be bound to restrict the source IP host to processing the initial packets in a TCP handshake, instead of conducting restriction after a TCP connection is established. The global control plane security ACL filters packets only through software. It not only reduces the hardware resource consumption but also meets the requirement for processing the initial TCP packets. If you apply a security ACL globally by running a control plane application command, the ACL takes effect on software only.

The global control plane security ACL takes effect on all L2 ports. ACEs are not applied to hardware but only to software, which reduces the hardware resource consumption. During a TCP handshake, the software ACL checks initial TCP packets and filters out the TCP packets that match the ACL.

Note

- The global control plane security ACL is effective to software-based filtering and can be applied only to the inbound direction.
- The global control plane security ACL is not limited by the configuration of global ACL excluded ports. After the excluded ports are configured, the global control plane security ACL remains effective on the excluded ports.
- The global control plane security ACL takes effect on both L2 ports and L3 ports. That is, it can take effect on the following types of ports: access port, trunk port, hybrid port, L3 Ethernet port, L2 or L3 aggregation port. It does not take effect on the SVIs or member ports of aggregation ports.
- The global control plane security ACL can be associated only with the IP standard ACL.

1.2 Configuration Task Summary

Select at least one of the following tasks to configure:

- Configuring an IP Standard ACL
- Configuring an IP Extended ACL
- Configuring a MAC Extended ACL
- Configuring an Expert Extended ACL
- Configuring an IPv6 ACL
- Configuring an Expert Advanced ACL (ACL80)

1.3 Configuring an IP Standard ACL

1.3.1 Overview

This section describes how to create and apply an IP standard ACL to control the IPv4 packets entering/leaving a port. You can deny or permit specific IPv4 packets destined to a network so as to control the access of IP users to network resources.

1.3.2 Restrictions and Guidelines

- If a device needs to control users' access to network resources by checking the source IP addresses of packets, you can configure an IP standard ACL.
- The IP standard ACL can be configured on access, convergence, or core devices, depending on user distribution. The IP standard ACL takes effect only on the configured device, and does not affect the other devices in the network.

1.3.3 Configuration Tasks

IP standard ACL configuration includes the following tasks:

(1) Creating an IP Standard ACL

(2) Applying an IP Standard ACL

(3) (Optional) Configuring a Global Security ACL

(4) (Optional) Configuring a Security Channel

(5) (Optional) Configuring a Redirect ACL

(6) (Optional) Configuring the Fragmented Packet Matching Mode

(7) (Optional) Configuring the SVI Router ACL

1.3.4 Creating an IP Standard ACL

1. Overview

This section describes how to create an IP standard ACL and configure rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all IPv4 packets from entering the device.
- To make some ACL rules take effect at specified time or expire at specified time, for example, make an ACL effective within some time ranges in a week, configure an ACL rule with the **time-range** option.
- When configuring an ACL rule with the **time-range** option, configure the time range option. For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".
- Configuring an ACL rule with the **log** option consumes more hardware resources. If all the configured rules have the **log** option, the hardware policy capacity of the device is halved.
- The default output interval of packet matching logs is 0 minutes, that is, no ACL matching log is output. After specifying the **log** option when configuring ACL rules, you also need to configure an output interval; otherwise no matching log is output.
- For a rule with the **log** option, if no packet is matched within the specified time interval, no packet matching log related to the rule is output; if a packet is matched within the specified time interval, the packet matching log related to the rule is output after the time interval expires. The number of matched packets is the total number of packets matching the rule within the time interval, that is, the number of matched packets from the last log output to the current log output.
- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.
- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an IP standard ACL and configure rules. Please configure only one task.

- Create a numerically indexed IP standard ACL and configure rules.

access-list *acl-number* { **permit** | **deny** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-name*]

[**log**]

- Create a numerically indexed or named IP standard ACL and configure rules. Run the following commands in turn to create an IP standard ACL and configure rules.

  ip access-list standard { *acl-number* | *acl-name* }

  No IP standard ACL is configured by default.

  Run the command to create an IP standard ACL and enter the IP standard ACL configuration mode.

  [*sn*] { **permit** | **deny** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-name*]

  [**log**]

  There is an ACL rule of deny type in an ACL by default.

(4) (Optional) Configure a remark for the ACL. Please configure only one task.

- Configure a remark for the numerically indexed IP standard ACL.

  access-list *acl-number* **list-remark** *comment*

- Configure remarks for rules in the numerically indexed or named IP standard ACL.

  list-remark *comment*

No remark is configured for an ACL by default.

(5) (Optional) Configure remarks for rules in the IP standard ACL. Please configure only one task.

- Configure remarks for rules in the numerically indexed IP standard ACL.

  access-list *acl-number* **remark** *comment*

- Configure remarks for rules in the numerically indexed or named IP standard ACL.

  remark *comment*

No remark is configured for ACL rules by default.

(6) (Optional) Configure an update interval of packet matching logs.

ip access-list log-update interval *time*

The default update interval of packet matching logs is 0 minutes, that is, no ACL matching log is output.

(7) (Optional) Configure a step for rule sequence numbers in the IP standard ACL.

ip access-list resequence { *acl-number* | *acl-name* } *start-sn inc-sn*

Both the start value and step of ACL rule sequence numbers are **10** by default.

1.3.5 Applying an IP Standard ACL

1. Overview

You can apply an IP standard ACL in global configuration mode or interface configuration mode of a device, or VLAN interface configuration mode to make the IP standard ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface

configuration mode, or VLAN interface configuration mode, you can apply an IP standard ACL.

- Configuring the **in** or **out** option indicates that the IP standard ACL takes effect for the packets entering the device or those forwarded by the device.
- Configuring the **reflect** option enables the reflexive ACL.
- Configure the **counter-only** option to count the packets with some characteristics. The counting function takes effect only for permit rules but not for deny rules in an ACL.
- After an ACL is used as a **counter-only** ACL, the counting function cannot be globally enabled for the ACL, and the ACL cannot be applied globally or on ports as a common ACL. That is, ACLs with the same *acl-number* or *acl-name* cannot be used as a **counter-only** ACL and a common ACL at the same time.
- If the **control-plane** option is configured, the ACL is effective for software only so as to save hardware resources.
- If the **forward-plane** option is configured, the ACL is effective for hardware only.
- If the **forward-control-plane** option is configured, the ACL is effective for both software and hardware.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

  interface *interface-type interface-number*

- Enter the VLAN interface configuration mode.

  interface vlan *vlan-id*

(4) Apply the IP standard ACL in interface configuration mode.

ip access-group { *acl-number* | *acl-name* } { **in** | **out** } [**counter-only** | **control-plane** | **forward-control-plane** | **forward-plane**]

Running the command enables the IP standard ACL to take effect in specified interface configuration mode, or VLAN interface configuration mode.

1.3.6 Configuring a Global Security ACL

1. Overview

Configuring the global security ACL function can prevent internal access to illegal websites or stop viruses from entering the internal network of an enterprise. In addition, excluded ports of the global security ACL can be configured to permit some special departments in an enterprise to access some external websites.

2. Restrictions and Guidelines

- To implement global protection of the internal network, first configure an ACL.
- You can configure the global security ACL function on an access, aggregation, or core device based on the

distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.

- An ACL can contain no rules. When no rule is configured, the global security ACL function is unavailable.
- Disabling the global security ACL function disables configured global security ACLs.
- Configuring a port as an excluded port disables the global security ACL on the port.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Disable the global security ACL function.

global access-group disable

The global security ACL function is not disabled by default.

(4) Configure a global security ACL.

ip access-group { *acl-number* | *acl-name* } **global** { **in** | **out** } [**control-plane** | **forward-control-plane** | **forward-plane**]

No global security ACL is configured by default.

(5) Enter the interface configuration mode.

interface *interface-type interface-number*

(6) (Optional) Configure the global security ACL to take effect on the port.

global access-group

A port is an excluded port of the global security ACL by default.

(7) (Optional) Configure the global security ACL of the IP type to take effect on the port.

no global ip access-group

A port is an excluded port of the global security ACL of the IP type by default.

1.3.7 Configuring a Security Channel

1. Overview

The security channel function enables the packets conforming to the security channel rules to bypass the access control related services. For example, IEEE 802.1x access control is enabled on a port of the uplink device connected to a user host, and a security channel can be configured to permit the user to log in to a site to download the authentication client before 802.1x authentication.

2. Restrictions and Guidelines

- To implement the security channel function, first configure an ACL.
- You can configure the security channel function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured in an ACL, the security channel function is

unavailable.

- To make a security channel take effect on a port, configure the security channel on the specified port only; to make a security channel globally, configure a security channel in global configuration mode.
- If you have configured a global security channel but want to disable the security channel on some ports, configure these ports as excluded ports of the global security channel.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a specified ACL as a security channel. Please configure only one task.

- Configure a global security channel.

  security global access-group { *acl-number* | *acl-name* }

  No global security channel is configured by default.

- Configure a security channel on a port. Run the following commands in turn to configure a security channel on a port.

  interface *interface-type interface-number*

  security access-group { *acl-number* | *acl-name* }

  No security channel is configured on a port by default.

(4) (Optional) Configure a port as an excluded port of the security channel.

security uplink enable

No port is configured as an excluded port of a security channel globally by default.

1.3.8 Configuring a Redirect ACL

1. Overview

This section describes how to configure the redirect ACL function on a specified port or globally, to redirect the matched packets entering the port or all the ports to a specified port for forwarding.

2. Restrictions and Guidelines

- To implement the redirect ACL function, configure an ACL first.
- You can configure the redirect ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- The redirect ACL function can be configured on an Ethernet port, aggregation port, or SVI only.
- The packet to be redirected must be an L2 forwarded packet (that is, if a packet is forwarded from VLAN 2 to VLAN 3, it cannot be redirected), and the destination port of redirection must be in the same VLAN as the source port.
- An ACL can contain no rules. If no rule is configured in an ACL, the redirect ACL function is unavailable.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a redirect ACL. Please configure only one task.

- Configure a redirect ACL on a port. Run the following commands in turn to configure a redirect ACL on a port.

  interface *interface-type interface-number*

  redirect destination interface *interface-type interface-number* **acl** { *acl-number* | *acl-name* } **in**

  No redirect ACL is configured on a port by default.

  After the command is executed, the incoming packets of a specified port that match the ACL rules are redirected to a destination port for forwarding.

1.3.9 Configuring the Fragmented Packet Matching Mode

1. Overview

This function can be configured to enable ACL to control fragmented packets more finely.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the fragmented packet matching mode.

ip access-list new-fragment-mode { *acl-number* | *acl-name* }

The fragmented packet matching mode of an IP standard ACL or IP extended ACL is the default matching mode by default.

1.3.10 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the SVI router ACL.

svi router-acls enable

1.4 Configuring an IP Extended ACL

1.4.1 Overview

This section describes how to create and apply an IP extended ACL to control the IPv4 packets entering/leaving a port. You can deny or permit specific IPv4 packets destined to a network so as to control the access of IP users to network resources.

1.4.2 Restrictions and Guidelines

- If a device needs to control users' access to network resources by checking the source IP addresses, destination IP addresses, protocol numbers, TCP/UDP source or destination port IDs of packets, you can configure an IP extended ACL.
- The IP extended ACL can be configured on access, convergence, or core devices, depending on user distribution. The IP extended ACL takes effect only on a configured device, but does not affect the other devices in the network.

1.4.3 Configuration Tasks

IP extended ACL configuration includes the following tasks:

(1) Creating an IP Extended ACL

(2) Applying an IP Extended ACL

(3) (Optional) Configuring a Global Security ACL

(4) (Optional) Configuring a Security Channel

(5) (Optional) Configuring a Redirect ACL

(6) (Optional) Configuring the Fragmented Packet Matching Mode

(7) (Optional) Configuring the SVI Router ACL

1.4.4 Creating an IP Extended ACL

1. Overview

This section describes how to create an IP extended ACL and configure its rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all IPv4 packets from entering the device.
- To make some ACL rules take effect at specified time or expire at specified time, for example, make an ACL effective within some time ranges in a week, configure an ACL rule with the **time-range** option.
- When configuring an ACL rule with the **time-range** option, configure the time range option. For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".
- Configuring an ACL rule with the **log** option consumes more hardware resources. If all the configured rules

have the **log** option, the hardware policy capacity of the device is halved.

- The default output interval of packet matching logs is 0 minutes, that is, no ACL matching log is output. After specifying the **log** option when configuring ACL rules, you also need to configure an output interval; otherwise no matching log is output.
- For a rule with the **log** option, if no packet is matched within the specified time interval, no packet matching log related to the rule is output; if a packet is matched within the specified time interval, the packet matching log related to the rule is output after the time interval expires. The number of matched packets is the total number of packets matching the rule within the time interval, that is, the number of matched packets from the last log output to the current log output.
- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.
- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an IP extended ACL and its rules. Please configure only one task.

- Configure a numerically indexed IP extended ACL and its rules.

  access-list *acl-number* { **permit** | **deny** } *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-name*]

  [**log**]

- Configure a numerically indexed or named IP extended ACL and its rules. Run the following commands in turn to configure an IP extended ACL and its rules.

  ip access-list extended { *acl-number* | *acl-name* }

  No IP extended ACL is configured by default.

  Run the command to configure an IP extended ACL and enter the IP extended ACL configuration mode.

  [*sn*] { **permit** | **deny** } *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-name*]

  [**log**]

  There is an ACL rule of deny type in an ACL by default.

(4) (Optional) Configure a remark for the IP extended ACL. Please configure only one task.

- Configure a remark for a numerically indexed IP extended ACL.

  access-list *acl-number* **list-remark** *comment*

- Configure a remark for a numerically indexed or named IP extended ACL.

list-remark *comment*

No remark is configured for an ACL by default.

(5) (Optional) Configure remarks for rules in the IP extended ACL. Please configure only one task.

- Configure remarks for rules in the numerically indexed IP extended ACL.

  access-list *acl-number* **remark** *comment*

- Configure remarks for rules in the numerically indexed or named ACL.

  remark *comment*

No remark is configured for ACL rules by default.

(6) (Optional) Configure an update interval of packet matching logs.

ip access-list log-update interval *time*

The default update interval of packet matching logs is 0 minutes, that is, no ACL matching log is output.

(7) (Optional) Configure a step for rule sequence numbers in the IP extended ACL.

ip access-list resequence { *acl-number* | *acl-name* } *start-sn inc-sn*

Both the start value and step of ACL rule sequence numbers are **10** by default.

1.4.5 Applying an IP Extended ACL

1. Overview

This section describes how to apply an IP extended ACL to a device in interface configuration mode, or VLAN interface configuration mode to make the IP extended ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface configuration mode, or VLAN interface configuration mode, you can apply an IP extended ACL.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.
- Configuring the **reflect** option enables the reflexive ACL.
- Configure the **counter-only** option to count the packets with some characteristics. The counting function takes effect only for permit rules but not for deny rules in an ACL.
- After an ACL is used as a **counter-only** ACL, the counting function cannot be globally enabled for the ACL, and the ACL cannot be applied globally or on ports as a common ACL. That is, ACLs with the same *acl-number* or *acl-name* cannot be used as a **counter-only** ACL and a common ACL at the same time.
- If the **control-plane** option is configured, the ACL is effective for software only so as to save hardware resources.
- If the **forward-plane** option is configured, the ACL is effective for hardware only.
- If the **forward-control-plane** option is configured, the ACL is effective for both software and hardware.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

  interface *interface-type interface-number*

- Enter the VLAN interface configuration mode.

  interface vlan *vlan-id*

(4) Apply an IP extended ACL in interface configuration mode.

ip access-group { *acl-number* **|** *acl-name* } { **in** | **out** } [**reflect** | **counter-only**| **control-plane** | **forward-control-plane** | **forward-plane**]

Running the command enables an IP extended ACL to take effect in the specified interface configuration mode, or VLAN interface configuration mode.

1.4.6 Configuring a Global Security ACL

1. Overview

Configuring the global security ACL function can prevent internal access to illegal websites or stop viruses from entering the internal network of an enterprise. In addition, excluded ports of the global security ACL can be configured to permit some special departments in an enterprise to access some external websites.

2. Restrictions and Guidelines

- To implement global protection of the internal network, first configure an ACL.
- You can configure the global security ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured, the global security ACL function is unavailable.
- Disabling the global security ACL function disables configured global security ACLs.
- Configuring a port as an excluded port disables the global security ACL on the port.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Disable the global security ACL function.

global access-group disable

The global security ACL function is not disabled by default.

(4) Configure a global security ACL.

ip access-group { *acl-number* | *acl-name* } **global** { **in** | **out** } [**control-plane** | **forward-control-plane** | **forward-plane**]

No global security ACL is configured by default.

(5) Enter the interface configuration mode.

interface *interface-type interface-number*

(6) (Optional) Configure the global security ACL to take effect on the port.

global access-group

A port is an excluded port of the global security ACL by default.

(7) (Optional) Configure the global security ACL of the IP type to take effect on the port.

global ip access-group

A port is an excluded port of the global security ACL of the IP type by default.

1.4.7 Configuring a Security Channel

1. Overview

The security channel function enables the packets conforming to the security channel rules to bypass the access control related services. For example, IEEE 802.1x access control is enabled on a port of the uplink device connected to a user host, and a security channel can be configured to permit the user to log in to a site to download the authentication client before 802.1x authentication.

2. Restrictions and Guidelines

- To implement the security channel function, first configure an ACL.
- You can configure the security channel function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured in an ACL, the security channel function is unavailable.
- To make a security channel take effect on a port, configure the security channel on the specified port only; to make a security channel globally, configure a security channel in global configuration mode.
- If you have configured a global security channel but want to disable the security channel on some ports, configure these ports as excluded ports of the global security channel.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a specified ACL as a security channel. Please configure only one task.

- Configure a global security channel.

  security global access-group { *acl-number* | *acl-name* }

  No global security channel is configured by default.

- Configure a security channel on a port. Run the following commands in turn to configure a security channel on a port.

  interface *interface-type interface-number*

  security access-group { *acl-number* | *acl-name* }

No security channel is configured on a port by default.

(4) (Optional) Configure a port as an excluded port of the security channel.

security uplink enable

No port is configured as an excluded port of a global security channel by default.

1.4.8 Configuring a Redirect ACL

1. Overview

This section describes how to configure the redirect ACL function on a specified port or globally, to redirect the matched packets entering the port or all the ports to a specified port for forwarding.

2. Restrictions and Guidelines

- To implement the redirect ACL function, configure an ACL first.
- You can configure the redirect ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- The redirect ACL function can be configured on an Ethernet port, aggregation port, or SVI only.
- The packet to be redirected must be an L2 forwarded packet (that is, if a packet is forwarded from VLAN 2 to VLAN 3, it cannot be redirected), and the destination port of redirection must be in the same VLAN as the source port.
- An ACL can contain no rules. If no rule is configured in an ACL, the redirect ACL function is unavailable.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a redirect ACL. Please configure only one task.

- Configure a redirect ACL on a port. Run the following commands in turn to configure a redirect ACL on a port.

  interface *interface-type interface-number*

  redirect destination interface *interface-type interface-number* **acl** { *acl-number* | *acl-name* } **in**

  No redirect ACL is configured on a port by default.

  After the command is executed, the incoming packets of a specified port that match the ACL rules are redirected to a destination port for forwarding.

1.4.9 Configuring the Fragmented Packet Matching Mode

1. Overview

This function can be configured to enable ACL to control fragmented packets more finely.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the fragmented packet matching mode.

ip access-list new-fragment-mode { *acl-number* | *acl-name* }

The fragmented packet matching mode of an IP standard ACL or IP extended ACL is the default matching mode by default.

1.4.10 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the SVI router ACL.

svi router-acls enable

1.5 Configuring a MAC Extended ACL

1.5.1 Overview

This section describes how to create and apply a MAC extended ACL to control the L2 packets entering/leaving a port. You can deny or permit specific L2 packets destined to a network so as to control the access of users to network resources based on the L2 packet headers.

1.5.2 Restrictions and Guidelines

- If a device needs to control users' access to network resources based on the L2 packet information (such as the MAC addresses of users' PCs), you can configure a MAC extended ACL.
- The MAC extended ACL can be configured on access, convergence, or core devices, depending on user distribution. The MAC extended ACL takes effect only on the configured device, but does not affect other devices in the network.

1.5.3 Configuration Tasks

MAC extended ACL configuration includes the following tasks:

(1) Creating a MAC Extended ACL

(2) Applying a MAC Extended ACL

(3) (Optional) Configuring a Security Channel

(4) (Optional) Configuring a Redirect ACL

(5) (Optional) Configuring the SVI Router ACL

1.5.4 Creating a MAC Extended ACL

1. Overview

This section describes how to create a MAC extended ACL and configure its rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all Ethernet L2 packets from entering the device.
- To make some ACL rules take effect at specified time or expire at specified time, for example, make an ACL effective within some time ranges in a week, configure an ACL rule with the **time-range** option.
- When configuring an ACL rule with the **time-range** option, configure the time range option. For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".
- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.
- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a MAC extended ACL and its rules. Please configure only one task.

- Configure a numerically indexed MAC extended ACL and its rules.

  access-list *acl-number* { **permit** | **deny** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** *cos-value* [**inner** *cos-value*]] [**time-range** *time-name*]

- Configure a numerically indexed or named MAC extended ACL and its rules. Run the following commands in turn to configure a MAC extended ACL and its rules.

  mac access-list extended { *acl-number* | *acl-name* }

  No MAC extended ACL is configured by default.

  Run the command to configure a MAC extended ACL and enter the MAC extended ACL configuration mode.

[*sn*] { **permit** | **deny** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** *cos-value* [**inner** *cos-value*]] [**time-range** *time-name*]

There is an ACL rule of deny type in an ACL by default.

(4) (Optional) Configure a remark for the ACL. Please configure only one task.

- Configure a remark for the numerically indexed ACL.

  access-list *acl-number* **list-remark** *comment*

- Configure remarks for rules in the numerically indexed or named ACL.

  list-remark *comment*

No remark is configured for an ACL by default.

(5) (Optional) Configure remarks for ACL rules. Please configure only one task.

- Configure remarks for rules in the numerically indexed ACL.

  access-list *acl-number* **remark** *comment*

- Configure remarks for rules in the numerically indexed or named ACL.

  remark *comment*

No remark is configured for ACL rules by default.

(6) (Optional) Configure a step for rule sequence numbers in the ACL.

mac access-list resequence { *acl-number* | *acl-name* } *start-sn inc-sn*

Both the start value and step of ACL rule sequence numbers are **10** by default.

1.5.5 Applying a MAC Extended ACL

1. Overview

This section describes how to apply a MAC extended ACL to a device in interface configuration mode, or VLAN interface configuration mode to make the MAC extended ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface configuration mode, or VLAN interface configuration mode, you can apply a MAC extended ACL.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.
- Configuring the **reflect** option enables the reflexive ACL.
- Configure the **counter-only** option to count the packets with some characteristics. The counting function takes effect only for permit rules but not for deny rules in an ACL.
- After an ACL is used as a **counter-only** ACL, the counting function cannot be globally enabled for the ACL, and the ACL cannot be applied globally or on ports as a common ACL. That is, ACLs with the same *acl-number* or *acl-name* cannot be used as a **counter-only** ACL and a common ACL at the same time.
- If the **control-plane** option is configured, the ACL is effective for software only so as to save hardware resources.
- If the **forward-plane** option is configured, the ACL is effective for hardware only.

- If the **forward-control-plane** option is configured, the ACL is effective for both software and hardware.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

  interface *interface-type interface-number*

- Enter the VLAN interface configuration mode.

  interface vlan *vlan-id*

(4) Apply a MAC extended ACL in interface configuration mode.

mac access-group { *acl-number* | *acl-name* } { **in** | **out** } [**counter-only** | **control-plane** | **forward-control-plane** | **forward-plane**]

Running the command enables a MAC extended ACL to take effect in the specified interface configuration mode, or VLAN interface configuration mode.

1.5.6 Configuring a Security Channel

1. Overview

The security channel function enables the packets conforming to the security channel rules to bypass the access control related services. For example, IEEE 802.1x access control is enabled on a port of the uplink device connected to a user host, and a security channel can be configured to permit the user to log in to a site to download the authentication client before 802.1x authentication.

2. Restrictions and Guidelines

- To implement the security channel function, first configure an ACL.
- You can configure the security channel function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured in an ACL, the security channel function is unavailable.
- To make a security channel take effect on a port, configure the security channel on the specified port only; to make a security channel globally, configure a security channel in global configuration mode.
- If you have configured a global security channel but want to disable the security channel on some ports, configure these ports as excluded ports of the global security channel.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a specified ACL as a security channel. Please configure only one task.

- Configure a global security channel.

  security global access-group { *acl-number* | *acl-name* }

  No global security channel is configured by default.

- Configure a security channel on a port. Run the following commands in turn to configure a security channel on a port.

  interface *interface-type interface-number*

  security access-group { *acl-number* | *acl-name* }

  No security channel is configured on a port by default.

(4) (Optional) Configure a port as an excluded port of the security channel.

security uplink enable

No port is configured as an excluded port of a security channel globally by default.

1.5.7 Configuring a Redirect ACL

1. Overview

This section describes how to configure the redirect ACL function on a specified port or globally, to redirect the matched packets entering the port or all the ports to a specified port for forwarding.

2. Restrictions and Guidelines

- To implement the redirect ACL function, configure an ACL first.
- You can configure the redirect ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- The redirect ACL function can be configured on an Ethernet port, aggregation port, or SVI only.
- The packet to be redirected must be an L2 forwarded packet (that is, if a packet is forwarded from VLAN 2 to VLAN 3, it cannot be redirected), and the destination port of redirection must be in the same VLAN as the source port.
- An ACL can contain no rules. If no rule is configured in an ACL, the redirect ACL function is unavailable.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a redirect ACL. Please configure only one task.

- Configure a redirect ACL on a port. Run the following commands in turn to configure a redirect ACL on a port.

  interface *interface-type interface-number*

  redirect destination interface *interface-type interface-number* **acl** { *acl-number* | *acl-name* } **in**

No redirect ACL is configured on a port by default.

After the command is executed, the incoming packets of a specified port that match the ACL rules are redirected to a destination port for forwarding.

1.5.8 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the SVI router ACL.

svi router-acls enable

1.6 Configuring an Expert Extended ACL

1.6.1 Overview

This section describes how to create and apply an expert extended ACL to control the packets entering/leaving the port. You can deny or permit specific packets destined to a network.

1.6.2 Restrictions and Guidelines

- If a device needs to control users' access to network resources by using IP ACL rules, MAC extended ACL rules, and VLANs in a mixed manner, you can configure an expert extended ACL.
- You can perform this configuration on an access, convergence, or core device based on the distribution of users. The configuration takes effect only on a configured device, but does not affect other devices in the network.

1.6.3 Configuration Tasks

Expert extended ACL configuration includes the following tasks:

(1) Creating an Expert Extended ACL

(2) Applying an Expert Extended ACL

(3) (Optional) Configuring a Global Security ACL

(4) (Optional) Configuring a Security Channel

(5) (Optional) Configuring a Redirect ACL

(6) (Optional) Configuring the Fragmented Packet Matching Mode

(7) (Optional) Configuring the SVI Router ACL

1.6.4 Creating an Expert Extended ACL

1. Overview

This section describes how to create an expert extended ACL and configure its rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all packets from entering the device.
- To make some ACL rules take effect at specified time or expire at specified time, for example, make an ACL effective within some time ranges in a week, configure an ACL rule with the **time-range** option.
- When configuring an ACL rule with the **time-range** option, configure the time range option. For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".
- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.
- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an expert extended ACL and its rules. Please configure only one task.

- Configure a numerically indexed expert extended ACL and its rules.

  access-list *acl-number* { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [[**VID** [*vlan-id*] [**inner** *vlan-id*]]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source*-mac-*address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-name*]

- Configure a numerically indexed or named expert extended ACL and its rules. Run the following commands in turn to configure an expert extended ACL and its rules.

  expert access-list extended { *acl-number* | *acl-name* }

  No expert extended ACL is configured by default.

  Run the command to configure an expert extended ACL and enter the expert extended ACL configuration mode.

  [*sn*] { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source*-mac-*address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-*

mac-wildcard | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*] [**fragment**] [**time-range** *time-name*]

There is an ACL rule of deny type in an ACL by default.

(4) (Optional) Configure a remark for the ACL. Please configure only one task.

- Configure a remark for the numerically indexed ACL.

  access-list *acl-number* **list-remark** *comment*

- Configure remarks for rules in the numerically indexed or named ACL.

  list-remark *comment*

No remark is configured for an ACL by default.

(5) (Optional) Configure remarks for ACL rules. Please configure only one task.

- Configure remarks for rules in the numerically indexed ACL.

  access-list *acl-number* **remark** *comment*

- Configure remarks for rules in the numerically indexed or named ACL.

  remark *comment*

No remark is configured for ACL rules by default.

(6) (Optional) Configure a step for rule sequence numbers in the ACL.

expert access-list resequence { *acl-number* | *acl-name* } *start-sn inc-sn*

Both the start value and step of ACL rule sequence numbers are **10** by default.

1.6.5 Applying an Expert Extended ACL

1. Overview

You can apply an expert extended ACL to a device in global configuration mode or interface configuration mode, or VLAN interface configuration mode to make the expert extended ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface configuration mode, or VLAN interface configuration mode, you can apply an expert extended ACL.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.
- Configuring the **reflect** option enables the reflexive ACL.
- Configure the **counter-only** option to count the packets with some characteristics. The counting function takes effect only for permit rules but not for deny rules in an ACL.
- After an ACL is used as a **counter-only** ACL, the counting function cannot be globally enabled for the ACL, and the ACL cannot be applied globally or on ports as a common ACL. That is, ACLs with the same *acl-number* or *acl-name* cannot be used as a **counter-only** ACL and a common ACL at the same time.
- If the **control-plane** option is configured, the ACL is effective for software only so as to save hardware resources.
- If the **forward-plane** option is configured, the ACL is effective for hardware only.
- If the **forward-control-plane** option is configured, the ACL is effective for both software and hardware.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

  interface *interface-type interface-number*

- Enter the VLAN interface configuration mode.

  interface vlan *vlan-id*

(4) Apply an expert extended ACL in interface configuration mode.

expert access-group { *acl-number* | *acl-name* } { **in** | **out** } [**counter-only** | **control-plane** | **forward-control-plane** | **forward-plane**]

Run the command to enable an expert extended ACL to take effect on a specified port.

1.6.6 Configuring a Global Security ACL

1. Overview

Configuring the global security ACL function can prevent internal access to illegal websites or stop viruses from entering the internal network of an enterprise. In addition, excluded ports of the global security ACL can be configured to permit some special departments in an enterprise to access some external websites.

2. Restrictions and Guidelines

- To implement global protection of the internal network, first configure an ACL.
- You can configure the global security ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured, the global security ACL function is unavailable.
- Disabling the global security ACL function disables configured global security ACLs.
- Configuring a port as an excluded port disables the global security ACL on the port.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Disable the global security ACL function.

global access-group disable

The global security ACL function is not disabled by default.

(4) Configure a global security ACL.

expert access-group { *acl-number* | *acl-name* } **global** { **in** | **out** } [**control-plan** | **forward-control-plane** | **forward-plane**]

No global security ACL is configured by default.

(5) Enter the interface configuration mode.

interface *interface-type interface-number*

(6) (Optional) Configure the global security ACL to take effect on the port.

global access-group

A port is an excluded port of the global security ACL by default.

1.6.7 Configuring a Security Channel

1. Overview

The security channel function enables the packets conforming to the security channel rules to bypass the access control related services. For example, IEEE 802.1x access control is enabled on a port of the uplink device connected to a user host, and a security channel can be configured to permit the user to log in to a site to download the authentication client before 802.1x authentication.

2. Restrictions and Guidelines

- To implement the security channel function, first configure an ACL.
- You can configure the security channel function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured in an ACL, the security channel function is unavailable.
- To make a security channel take effect on a port, configure the security channel on the specified port only; to make a security channel globally, configure a security channel in global configuration mode.
- If you have configured a global security channel but want to disable the security channel on some ports, configure these ports as excluded ports of the global security channel.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a specified ACL as a security channel. Please configure only one task.

- Configure a global security channel.

  security global access-group { *acl-number* | *acl-name* }

  No global security channel is configured by default.

- Configure a security channel on a port. Run the following commands in turn to configure a security channel on a port.

  interface *interface-type interface-number*

security access-group { *acl-number* | *acl-name* }

No security channel is configured on a port by default.

(4) (Optional) Configure a port as an excluded port of the security channel.

security uplink enable

No port is configured as an excluded port of a security channel globally by default.

1.6.8 Configuring a Redirect ACL

1. Overview

This section describes how to configure the redirect ACL function on a specified port or globally, to redirect the matched packets entering the port or all the ports to a specified port for forwarding.

2. Restrictions and Guidelines

- To implement the redirect ACL function, configure an ACL first.
- You can configure the redirect ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- The redirect ACL function can be configured on an Ethernet port, aggregation port, or SVI only.
- The packet to be redirected must be an L2 forwarded packet (that is, if a packet is forwarded from VLAN 2 to VLAN 3, it cannot be redirected), and the destination port of redirection must be in the same VLAN as the source port.
- An ACL can contain no rules. If no rule is configured in an ACL, the redirect ACL function is unavailable.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a redirect ACL. Please configure only one task.

- Configure a redirect ACL on a port. Run the following commands in turn to configure a redirect ACL on a port.

  interface *interface-type interface-number*

  redirect destination interface *interface-type interface-number* **acl** { *acl-number* | *acl-name* } **in**

  No redirect ACL is configured on a port by default.

  After the command is executed, the incoming packets of a specified port that match the ACL rules are redirected to a destination port for forwarding.

1.6.9 Configuring the Fragmented Packet Matching Mode

1. Overview

This function can be configured to enable ACL to control fragmented packets more finely.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the fragmented packet matching mode.

expert access-list new-fragment-mode { *acl-number* | *acl-name* }

1.6.10 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the SVI router ACL.

svi router-acls enable

1.7 Configuring an IPv6 ACL

1.7.1 Overview

This section describes how to create and apply an IPv6 ACL to control the IPv6 packets entering/leaving the port. You can deny or permit specific IPv6 packets destined to a network so as to control the access of IPv6 users to network resources.

1.7.2 Restrictions and Guidelines

- To control IPv6 users' access to network resources, configure an IPv6 ACL.
- You can perform this configuration on an access, convergence, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.

1.7.3 Configuration Tasks

IPv6 ACL configuration includes the following tasks:

(1) Creating an IPv6 ACL

(2) Applying an IPv6 ACL

(3) (Optional) Configuring a Global Security ACL

(4) (Optional) Configuring a Security Channel

(5) (Optional) Configuring a Redirect ACL

(6) (Optional) Configuring the SVI Router ACL

1.7.4 Creating an IPv6 ACL

1. Overview

This section describes how to create an IPv6 ACL and configure its rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all IPv6 packets from entering the device.
- To make some ACL rules take effect at specified time or expire at specified time, for example, make an ACL effective within some time ranges in a week, configure an ACL rule with the **time-range** option.
- When configuring an ACL rule with the **time-range** option, configure the time range option. For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".
- Configuring an ACL rule with the **log** option consumes more hardware resources. If all the configured rules have the **log** option, the hardware policy capacity of the device is halved.
- The default output interval of packet matching logs is 0 minutes, that is, no ACL matching log is output. After specifying the **log** option when configuring ACL rules, you also need to configure an output interval; otherwise no matching log is output.
- For a rule with the **log** option, if no packet is matched within the specified time interval, no packet matching log related to the rule is output; if a packet is matched within the specified time interval, the packet matching log related to the rule is output after the time interval expires. The number of matched packets is the total number of packets matching the rule within the time interval, that is, the number of matched packets from the last log output to the current log output.
- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.
- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an IPv6 ACL and enter the IPv6 ACL configuration mode.

ipv6 access-list *acl-name*

No IPv6 ACL is configured by default.

(4) Configure IPv6 ACL rules. Please configure only one task.

- Configure IPv6 ACL rules of TCP or UDP.

[*sn*] { **permit** | **deny** } [*protocol* { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [*op dstport*] [**cos** *value* [**inner** *value*]] [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination-mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**vid** *vlan-id*] [**time-range** *time-name*] [**log**]

- Configure IPv6 ACL rules of protocols other than TCP or UDP.

  [*sn*] { **permit** | **deny** } [*protocol* { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** }] [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**vid** *vlan-id*] [**time-range** *time-name*] [**log**]

(5) (Optional) Configure a remark for the ACL.

list-remark *comment*

No remark is configured for an ACL by default.

(6) (Optional) Configure remarks for ACL rules.

remark *comment*

No remark is configured for ACL rules by default.

(7) (Optional) Configure an update interval of packet matching logs.

ipv6 access-list log-update interval *time*

The default update interval of packet matching logs is 0 minutes, that is, no ACL matching log is output.

(8) (Optional) Configure a step for rule sequence numbers in the ACL.

ipv6 access-list resequence *acl-name start-sn inc-sn*

Both the start value and step of ACL rule sequence numbers are **10** by default.

1.7.5 Applying an IPv6 ACL

1. Overview

This section describes how to apply an IPv6 ACL to a device in interface configuration mode, or VLAN interface configuration mode to make the IPv6 ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface configuration mode, or VLAN interface configuration mode, you can apply an IPv6 ACL.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.
- Configuring the **reflect** option enables the reflexive ACL.
- Configure the **counter-only** option to count the packets with some characteristics. The counting function takes effect only for permit rules but not for deny rules in an ACL.
- After an ACL is used as a **counter-only** ACL, the counting function cannot be globally enabled for the ACL,

and the ACL cannot be applied globally or on ports as a common ACL. That is, ACLs with the same *acl-number* or *acl-name* cannot be used as a **counter-only** ACL and a common ACL at the same time.

- If the **control-plane** option is configured, the ACL is effective for software only so as to save hardware resources.
- If the **forward-plane** option is configured, the ACL is effective for hardware only.
- If the **forward-control-plane** option is configured, the ACL is effective for both software and hardware.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

  interface *interface-type interface-number*

- Enter the VLAN interface configuration mode.

  interface vlan *vlan-id*

(4) Apply an IPv6 ACL in interface configuration mode.

ipv6 traffic-filter *acl-name* { **in** | **out** } [**counter-only** | **control-plane** | **forward-control-plane** | **forward-plane**]

Run the command to enable an IPv6 ACL to take effect in global configuration mode or specified interface configuration mode, or VLAN interface configuration mode.

1.7.6 Configuring a Global Security ACL

1. Overview

Configuring the global security ACL function can prevent internal access to illegal websites or stop viruses from entering the internal network of an enterprise. In addition, excluded ports of the global security ACL can be configured to permit some special departments in an enterprise to access some external websites.

2. Restrictions and Guidelines

- To implement global protection of the internal network, first configure an ACL.
- You can configure the global security ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured, the global security ACL function is unavailable.
- Disabling the global security ACL function disables configured global security ACLs.
- Configuring a port as an excluded port disables the global security ACL on the port.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Disable the global security ACL function.

global access-group disable

The global security ACL function is not disabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) (Optional) Configure the global security ACL to take effect on the port.

global access-group

A port is an excluded port of the global security ACL by default.

1.7.7 Configuring a Security Channel

1. Overview

The security channel function enables the packets conforming to the security channel rules to bypass the access control related services. For example, IEEE 802.1x access control is enabled on a port of the uplink device connected to a user host, and a security channel can be configured to permit the user to log in to a site to download the authentication client before 802.1x authentication.

2. Restrictions and Guidelines

- To implement the security channel function, first configure an ACL.
- You can configure the security channel function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured in an ACL, the security channel function is unavailable.
- To make a security channel take effect on a port, configure the security channel on the specified port only; to make a security channel globally, configure a security channel in global configuration mode.
- If you have configured a global security channel but want to disable the security channel on some ports, configure these ports as excluded ports of the global security channel.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a specified ACL as a security channel. Please configure only one task.

- Configure a global security channel.

  security global access-group *acl-name*

  No global security channel is configured by default.

- Configure a security channel on a port. Run the following commands in turn to configure a security channel on a port.

  interface *interface-type interface-number*

  security access-group *acl-name*

  No security channel is configured on a port by default.

(4) (Optional) Configure a port as an excluded port of the security channel.

security uplink enable

No port is configured as an excluded port of a security channel globally by default.

1.7.8 Configuring a Redirect ACL

1. Overview

This section describes how to configure the redirect ACL function on a specified port or globally, to redirect the matched packets entering the port or all the ports to a specified port for forwarding.

2. Restrictions and Guidelines

- To implement the redirect ACL function, configure an ACL first.
- You can configure the redirect ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- The redirect ACL function can be configured on an Ethernet port, aggregation port, or SVI only.
- The packet to be redirected must be an L2 forwarded packet (that is, if a packet is forwarded from VLAN 2 to VLAN 3, it cannot be redirected), and the destination port of redirection must be in the same VLAN as the source port.
- An ACL can contain no rules. If no rule is configured in an ACL, the redirect ACL function is unavailable.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a redirect ACL. Please configure only one task.

- Configure a redirect ACL on a port. Run the following commands in turn to configure a redirect ACL on a port.

  interface *interface-type interface-number*

  redirect destination interface *interface-type interface-number* **acl** *acl-name* **in**

  No redirect ACL is configured on a port by default.

  After the command is executed, the incoming packets of a specified port that match the ACL rules are redirected to a destination port for forwarding.

1.7.9 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the SVI router ACL.

svi router-acls enable

1.8 Configuring an Expert Advanced ACL (ACL80)

1.8.1 Overview

When the fixed matching fields of the IP standard ACL, IP extended ACL, MAC extended ACL, expert extended ACL, and IPv6 ACL all fail to meet requirements, you can configure an ACL80 to define the packet fields to be matched.

1.8.2 Restrictions and Guidelines

- To implement the ACL80 function, first configure an expert advanced ACL.
- You can perform this configuration on an access, convergence, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.

1.8.3 Configuration Tasks

The ACL80 configuration includes the following tasks:

(1) Creating an ACL80

(2) Applying an ACL80

(3) (Optional) Configuring the SVI Router ACL

1.8.4 Creating an ACL80

1. Overview

This section describes how to create an ACL80 and configure its rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all packets from entering the device.

- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.
- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an expert advanced ACL and enter the expert advanced ACL configuration mode.

expert access-list advanced *acl-name*

No expert advanced ACL is configured by default.

(4) (Optional) Configure rules in the expert advanced ACL.

[*sn*] { **permit** | **deny** } *hex hex-mask offset*

Run the command to configure user-defined rules for an ACL in expert advanced ACL mode.

(5) (Optional) Configure a remark for the ACL.

list-remark *comment*

No remark is configured for an ACL by default.

(6) (Optional) Configure remarks for ACL rules.

remark *comment*

No remark is configured for ACL rules by default.

1.8.5 Applying an ACL80

1. Overview

This section describes how to apply an expert advanced ACL to a device in interface configuration mode, or VLAN interface configuration mode to make the expert advanced ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface configuration mode, or VLAN interface configuration mode, you can apply an expert advanced ACL.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

  interface *interface-type interface-number*

- Enter the VLAN interface configuration mode.

  interface vlan *vlan-id*

(4) Apply an expert advanced ACL in interface configuration mode.

expert access-group { *acl-number* | *acl-name* } { **in** | **out** }

1.8.6 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the SVI router ACL.

svi router-acls enable

1.9 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

Running the **clear** commands may interrupt services due to loss of important information.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-5 ACL Monitoring

Command	Purpose
show access-lists [*acl-number* | *acl-ame*] [**summary**]	Displays a basic ACL.
show redirect [**interface** *interface-type interface-number*]	Displays the redirection entries bound to a specified port. If no port is specified, the redirection entries bound to all the ports are displayed.
show access-group [**interface** *interface-type interface-number* | **vlan** *vlan-id*]	Displays the configuration of an ACL applied to a port.
show ip access-group [**interface** *interface-type interface-number* | **vlan** *vlan-id*]	Displays the configuration of an IP standard ACL and an extended ACL applied to a port.
show mac access-group [**interface** *interface-type interface-number* | **vlan** *vlan-id*]	Displays the configuration of a MAC extended ACL applied to a port.
show expert access-group [**interface** *interface-type interface-number* | **vlan** *vlan-id*]	Displays the configuration of an expert extended ACL applied to a port.
show ipv6 traffic-filter [**interface** *interface-type interface-number* | **vlan** *vlan-id*]	Displays the configuration of an IPv6 ACL applied to a port.
show acl res [**dev** *dev-num* [**slot** *slot-num*]]	Displays information about all ternary content-addressable memory (TCAMs) or a specified TCAM.
show svi router-acls state	Checks whether an ACL applied to an SVI takes effect on L2 and L packets.
show qos res [**dev** *dev-num* [**slot** *slot-num*]]	Displays information about all the QoS resources or a specified QoS resource.
show acl res detail [**dev** *dev-num* [**slot** *slot-num*]]	Displays usage details about all TCAMs or a specified TCAM.
clear counters access-list [*acl-number* | *acl-name*]	Clears the number of packets matching an ACL.
clear access-list counters [*acl-number* | *acl-name*]	Clears the number of packets matching ACL deny rules.
debug acl acld event	Debugs the ACL running process.
debug acl acld client-show	Displays ACL client information.
debug acl acld acl-show	Displays ACLs created on all ACL clients.

1.10 Examples

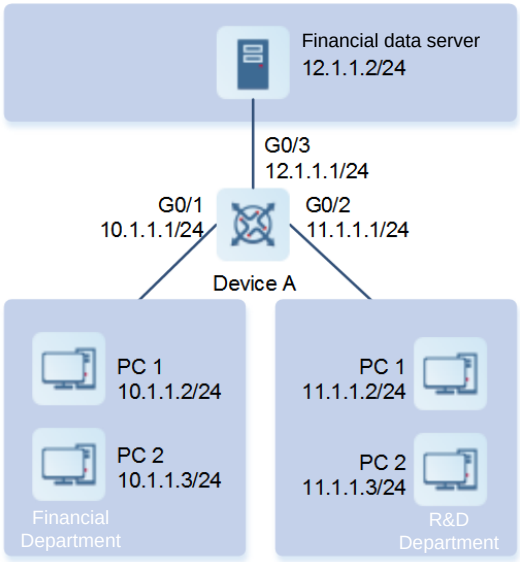
1.10.1 Configuring an IP Standard ACL

1. Requirements

An IP standard ACL needs to be configured to prevent the departments other than the financial department from accessing the financial data server.

2. Topology

Figure 1-3 Topology of IP Standard ACL Application Scenario



3. Notes

- Configure an IP standard ACL on device A and add access rules.
- Apply the IP standard ACL to the outbound direction of the port connected to the financial data server on device A.

4. Procedure

(1) Configure an IP standard ACL and add access rules.

On device A, configure an IP standard ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip access-list standard 1
DeviceA(config-std-nacl)# permit 10.1.1.0 0.0.0.255
DeviceA(config-std-nacl)# deny 11.1.1.1 0.0.0.255
DeviceA(config-std-nacl)# exit
```

(2) Apply the IP standard ACL to a port.

On device A, apply the IP standard ACL to the outbound direction of the port connected to the financial data server.

```
DeviceA(config)# interface gigabitethernet 0/3
DeviceA(config-if-GigabitEthernet 0/3)# ip access-group 1 out
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA# show access-lists

ip access-list standard 1
10 permit 10.1.1.0 0.0.0.255
20 deny 11.1.1.0 0.0.0.255

DeviceA# show access-group
ip access-group 1 out
Applied On interface GigabitEthernet 0/3
```

Ping the financial data server from a PC of the R&D department and confirm that the ping operation fails.

Ping the financial data server from a PC of the financial department and confirm that the ping operation succeeds.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
ip access-list standard 1
 10 permit 10.1.1.0 0.0.0.255
 20 deny 11.1.1.0 0.0.0.255
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 11.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip access-group 1 out
 ip address 12.1.1.1 255.255.255.0
!
```

1.10.2 Configuring an IP Extended ACL

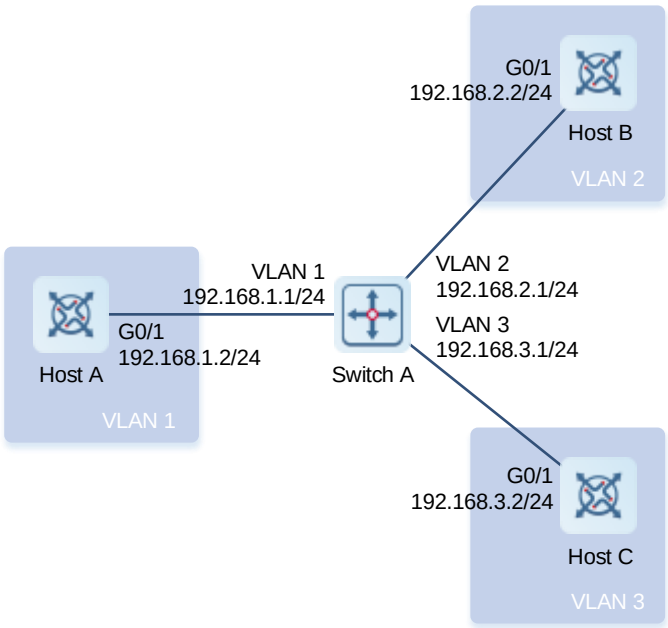
1. Requirements

Host A (VLAN 1), host B (VLAN 2), and host C (VLAN 3) are directly connected to the device which functions as the gateway of all the hosts. Requirement 1: The ping operation fails between VLAN 2 and VLAN 3, but succeeds between VLAN 1 and VLAN 2, and between VLAN 1 and VLAN 3. Requirement 2: The DHCP packets of VLAN

1 and VLAN 2 are unreachable to each other, but the communication using other protocols is normal. Requirement 3: The host in VLAN 1 cannot to access VLAN 3 through telnet or SSH, but the communication using other protocols is normal.

2. Topology

Figure 1-4 Topology of IP Extended ACL Application Scenario



3. Notes

- On switch A, configure an IP extended ACL and add an access rule of filtering out packets received by UDP port 67 or 68 to meet requirement 2. On host C, configure an IP extended ACL and add an access rule of filtering out packets received by ACL ports 23 and 22 to meet requirement 3.
- On switch A, apply the IP extended ACL to VLAN 1 interface, VLAN 2 interface, and VLAN 3 interface. On host C, apply the IP extended ACL to the line connected to the device.

4. Procedure

(1) Configure IP addresses for all the device ports (omitted).

(2) Configure an IP extended ACL and add access rules.

On switch A, configure an IP extended ACL and add access rules.

```
SwitchA> enable
SwitchA# configure terminal
SwitchA(config)# ip access-list extended inter_vlan_access1
SwitchA(config-ext-nacl)# deny udp any eq bootps any eq bootpc
SwitchA(config-ext-nacl)# deny udp any eq bootpc any eq bootps
SwitchA(config-ext-nacl)# remark //Deny DHCP packets.
SwitchA(config-ext-nacl)# permit ip any any
SwitchA(config-ext-nacl)# remark //Permit the communication using other
packets.
```

```
SwitchA(config-ext-nacl)# exit
SwitchA(config)# ip access-list extended inter_vlan_access2
SwitchA(config-ext-nacl)# deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
SwitchA(config-ext-nacl)# remark //Deny the mutual access between VLAN 2 and
VLAN 3.
SwitchA(config-ext-nacl)# deny udp any eq bootpc any eq bootps
SwitchA(config-ext-nacl)# deny udp any eq bootps any eq bootpc
SwitchA(config-ext-nacl)# remark //Deny DHCP packets.
SwitchA(config-ext-nacl)# permit ip any any
SwitchA(config-ext-nacl)# remark //Permit the communication using other
packets.
SwitchA(config-ext-nacl)# exit
SwitchA(config)# ip access-list extended inter_vlan_access3
SwitchA(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
SwitchA(config-ext-nacl)# remark //Deny the mutual access between VLAN 2 and
VLAN 3.
SwitchA(config-ext-nacl)# permit ip any any
SwitchA(config-ext-nacl)# remark //Permit the communication using other
packets.
SwitchA(config-ext-nacl)# exit
```

On host C, configure an IP extended ACL and add access rules.

```
HostC> enable
HostC# configure terminal
HostC(config)# ip access-list extended access_deny
HostC(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 eq telnet any eq telnet
HostC(config-ext-nacl)# remark //Deny VLAN 1 access to VLAN 3 through telnet.
HostC(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 eq 22 any eq 22
HostC(config-ext-nacl)# remark //Deny VLAN 1 access to VLAN 3 through SSH.
HostC(config-ext-nacl)# exit
```

(3) Apply the IP extended ACLs.

On switch A, apply the IP extended ACL to the corresponding ports.

```
SwitchA(config)# interface vlan 1
SwitchA(config-if-VLAN 1)# ip access-group inter_vlan_access1 in
SwitchA(config-if-VLAN 1)# exit
SwitchA(config)# interface vlan 2
SwitchA(config-if-VLAN 2)# ip access-group inter_vlan_access2 in
SwitchA(config-if-VLAN 2)# exit
SwitchA(config)# interface vlan 3
SwitchA(config-if-VLAN 3)# ip access-group inter_vlan_access3 in
SwitchA(config-if-VLAN 3)# exit
```

On host C, apply the IP extended ACL to the line connected to the device.

```
hostC(config)# line vty 0
hostC(config-line)# access-class access_deny in
hostC(config-line)# exit
```

5. Verification

(1) Verify the connectivity.

The ping operation succeeds between VLAN 1 and VLAN 2, and between VLAN 1 and VLAN 3.

```
hostA# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/10 ms
hostA#
hostA# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/10 ms
```

The ping operation fails between VLAN 2 and VLAN 3.

```
hostB# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5)
```

(2) The host in VLAN 1 cannot access VLAN 3 through telnet.

```
hostA# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/10 ms
hostA#
hostA# telnet 192.168.3.2
Trying 192.168.3.2, 23...
% Destination unreachable; gateway or host down
```

6. Configuration Files

- Switch A configuration file

```
hostname SwitchA
!
vlan 1
!
vlan 2
!
vlan 3
!
ip access-list extended inter_vlan_access1
 10 deny udp any eq bootps any eq bootpc
 20 deny udp any eq bootpc any eq bootps
```

```
 remark //Deny DHCP packets.
 30 permit ip any any
 remark //Permit the communication using other packets.
!
ip access-list extended inter_vlan_access2
 10 deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
 remark //Deny the mutual access between VLAN 2 and VLAN 3.
 20 deny udp any eq bootpc any eq bootps
 30 deny udp any eq bootps any eq bootpc
 remark //Deny DHCP packets.
 40 permit ip any any
 remark //Permit the communication using other packets.
!
ip access-list extended inter_vlan_access3
 10 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
 remark //Deny the mutual access between VLAN 2 and VLAN 3.
 20 permit ip any any
 remark //Permit the communication using other packets.
!
interface GigabitEthernet 1/0
 switchport access vlan 1
 description link_to_hostA
!
interface GigabitEthernet 1/1
 switchport access vlan 2
 description link_to_hostB
!
interface GigabitEthernet 1/2
 switchport access vlan 3
 description link_to_hostC
!
interface VLAN 1
 ip access-group inter_vlan_access1 in
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 2
 ip access-group inter_vlan_access2 in
 ip address 192.168.2.1 255.255.255.0
!
interface VLAN 3
 ip access-group inter_vlan_access3 in
 ip address 192.168.3.1 255.255.255.0
!
```

- Host A configuration file

```
hostname HostA
```

```
!
interface GigabitEthernet 0/1
 ip address 192.168.1.2 255.255.255.0
!
```

- Host B configuration file

```
hostname HostB
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
!
```

- Host C configuration file

```
hostname HostC
!
ip access-list extended access_deny
 10 deny tcp 192.168.1.0 0.0.0.255 eq telnet any eq telnet
 remark //Denies VLAN 1 access to VLAN 3 through telnet.
 20 deny tcp 192.168.1.0 0.0.0.255 eq 22 any eq 22
 remark //Deny VLAN 1 access to VLAN 3 through SSH.
!
interface GigabitEthernet 0/1
 ip address 192.168.3.2 255.255.255.0
!
line vty 0
 access-class access_deny in
 login
 password ruijie
!
```

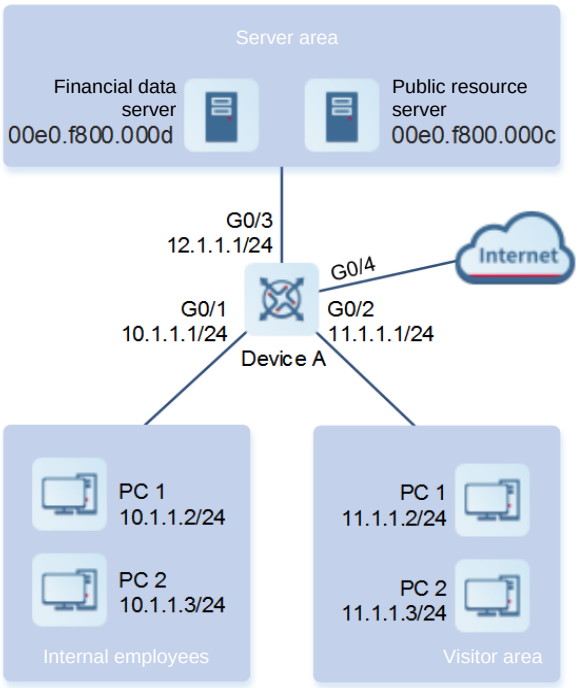
1.10.3 Configuring a MAC Extended ACL

1. Requirements

A MAC extended ACL needs to be configured to restrict the resources accessible to visitors.

2. Topology

Figure 1-5 Topology of MAC Extended ACL Application Scenario



3. Notes

- On device A, configure a MAC extended ACL and add access rules. The PCs in the visitor area are allowed to access the Internet and the company's internal public server, but are not allowed to access the company's financial data server, that is, the PCs are prohibited from accessing the server with MAC address 00e0.f800.000d.
- On device A, apply the MAC extended ACL to the inbound direction of a port connected to the visitor area.

4. Procedure

(1) Configure a MAC extended ACL and add access rules.

On device A, configure a MAC extended ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# mac access-list extended 700
DeviceA(config-mac-nacl)# deny any host 00e0.f800.000d
DeviceA(config-mac-nacl)# permit any any
DeviceA(config-mac-nacl)# exit
```

(2) Apply the MAC extended ACL to a port.

On device A, apply the ACL to the inbound direction of the port connected to the visitor area.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# mac access-group 700 in
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA# show access-lists
mac access-list extended 700
10 deny any host 00e0.f800.000d etype-any
20 permit any any etype-any
DeviceA# show access-group
mac access-group 700 in
Applied On interface GigabitEthernet 0/2
```

Ping the financial data server from a visitor PC and confirm that the ping operation fails.

Ping the public resource server from a visitor PC and confirm that the ping operation succeeds.

Access the Internet through a visitor PC, for example, access www.baidu.com, and confirm that the home page can be opened.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
mac access-list extended 700
 10 deny any host 00e0.f800.000d
 20 permit any any
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 mac access-group 700 in
 ip address 11.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip address 12.1.1.1 255.255.255.0
!
```

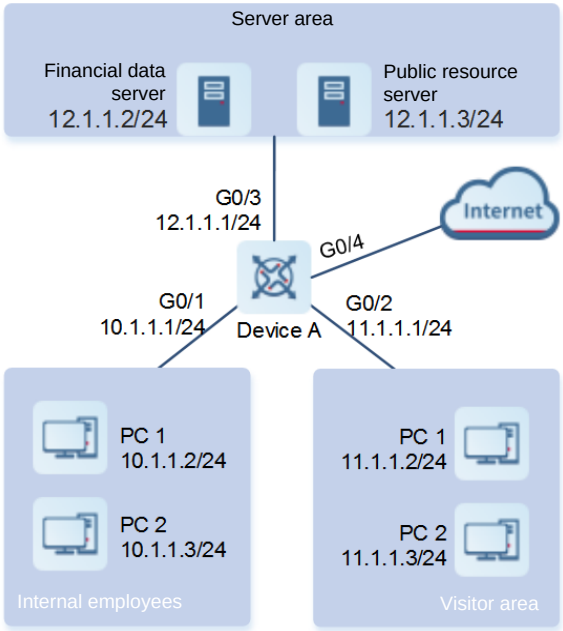
1.10.4 Configuring an Expert Extended ACL

1. Requirements

An expert extended ACL needs to be configured to restrict the resources accessible to visitors. Visitors cannot access the PCs of internal employees or the financial data server of the company, but can access the public resource server.

2. Topology

Figure 1-6 Topology of Expert Extended ACL Application Scenario



3. Notes

- On device A, configure an expert extended ACL and add access rules, including:
  - Prohibiting the hosts in the visitor area from sending packets destined to the network segment of internal employees' PCs.
  - Prohibiting visitors from accessing the financial data server.
  - Permitting all the other packets to pass through.
- On device A, apply the ACL to the inbound direction of the port connected to the visitor area.

4. Procedure

(1) Configure an expert extended ACL and add access rules.

On device A, configure an expert extended ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# expert access-list extended 2700
DeviceA(config-exp-nacl)# deny ip any any 10.1.1.0 0.0.0.255 any
DeviceA(config-exp-nacl)# deny ip any any host 12.1.1.2 any
DeviceA(config-exp-nacl)# permit any any any any
DeviceA(config-exp-nacl)# exit
```

(2) Apply the expert extended ACL to a port.

On device A, apply the ACL to the inbound direction of the port connected to the visitor area.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# expert access-group 2700 in
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA(config)# show access-lists
expert access-list extended 2700
 10 deny ip any any 192.168.1.0 0.0.0.255 any
20 deny ip any any host 10.1.1.1 any
30 permit ip any any any any

DeviceA(config)# show access-group
expert access-group 2700in
Applied On interface GigabitEthernet 0/2
```

Ping the financial data server from a visitor PC and confirm that the ping operation fails.

Ping the public resource server from a visitor PC and confirm that the ping operation fails.

Ping the internal employee gateway 192.168.1.1 from a visitor PC and confirm that the ping operation fails.

Access the Internet through a visitor PC, for example, access www.baidu.com, and confirm that the home page can be opened.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
expert access-list extended 2700
 10 deny ip any any 10.1.1.0 0.0.0.255 any
 20 deny ip any any host 12.1.1.2 any
 30 permit ip any any any any
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 expert access-group 2700 in
 ip address 11.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip address 12.1.1.1 255.255.255.0
!
```

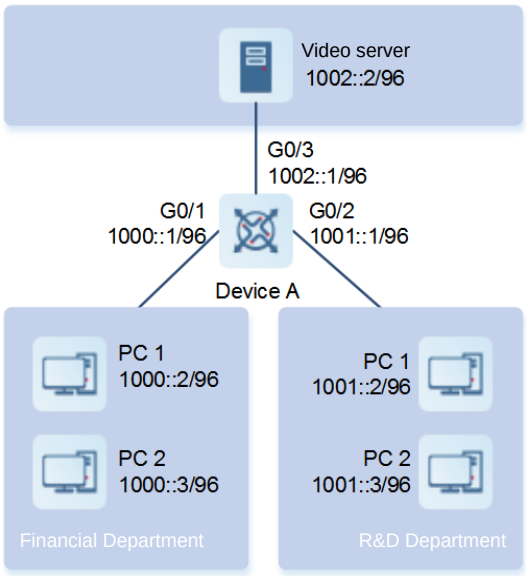
1.10.5 Configuring an IPv6 ACL

1. Requirements

An IPv6 ACL needs to be configured to prevent hosts in the R&D department from accessing the video server.

2. Topology

Figure 1-7 Topology of IPv6 ACL Application Scenario



3. Notes

- On device A, configure an IPv6 ACL and add access rules, including:
  - Prohibiting access to the IPv6 address of the video server.
  - Permitting all the IPv6 packets to pass through.
- On device A, apply the IPv6 ACL to the inbound direction of the port connected to the R&D department.

4. Procedure

(1) Configure an IPv6 ACL and add access rules.

On device A, configure an IPv6 ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ipv6 access-list dev_deny_ipv6video
DeviceA(config-ipv6-nacl)# deny ipv6 any host 1002::2
DeviceA(config-ipv6-nacl)# permit ipv6 any any
DeviceA(config-ipv6-nacl)# exit
```

(2) Apply the IPv6 ACL to a port.

On device A, apply the ACL to the inbound direction of the port connected to the R&D department.

```
DeviceA(config)# interface gigabitethernet 0/2
```

```
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 traffic-filter dev_deny_ipv6video
in
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA(config)# show access-lists

ipv6 access-list dev_deny_ipv6video
10 deny ipv6 any host 200::1
20 permit ipv6 any any

DeviceA(config)# show access-group
ipv6 traffic-filter dev_deny_ipv6video in
Applied On interface GigabitEthernet 0/2
```

Ping the video server from a PC in the R&D department and confirm that the ping operation fails.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
ipv6 access-list dev_deny_ipv6video
 10 deny ipv6 any host 1002::2
 20 permit ipv6 any any
!
interface GigabitEthernet 0/1
 no switchport
 ipv6 address 1000::1/96
!
interface GigabitEthernet 0/2
 no switchport
 ipv6 traffic-filter dev_deny_ipv6video in
 ipv6 address 1001::1/96
!
interface GigabitEthernet 0/3
 no switchport
 ipv6 address 1002::1/96
!
```

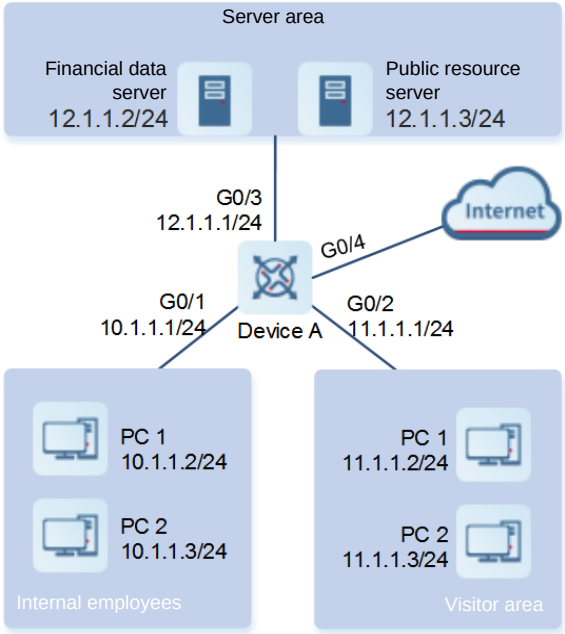
1.10.6 Configuring an ACL80

1. Requirements

An ACL80, namely, an expert advanced ACL needs to be configured to restrict the resources accessible by visitors. Visitors cannot access the PCs of internal employees or the financial data server of the company, but can access the public resource server.

2. Topology

Figure 1-8 Topology of ACL80 Application Scenario



3. Notes

- On device A, configure an expert advanced ACL and add access rules, including:
  - Prohibiting the hosts in the visitor area from sending packets destined to the network segment of internal employees' PCs.
  - Prohibiting visitors from accessing the financial data server.
  - Permitting all the other packets to pass through.
- On device A, apply the ACL to the inbound direction of the port connected to the visitor area.

4. Procedure

(1) Configure an expert advanced ACL and add access rules.

On device A, configure an expert advanced ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# expert access-list advanced acl80-guest
DeviceA(config-exp-dacl)# deny 0800 FFFF 24 0A0101 FFFFFF 42
DeviceA(config-exp-dacl)# deny 0800 FFFF 24 0C010102 FFFFFFFF 42
DeviceA(config-exp-dacl)# permit 0806 FFFF 24
DeviceA(config-exp-dacl)# permit 0800 FFFF 24
DeviceA(config-exp-dacl)# exit
```

(2) Apply the expert advanced ACL to a port.

On device A, apply the ACL80 to the inbound direction of the port connected to the visitor area.

```
DeviceA(config)# interface gigabitethernet 0/2
```

```
DeviceA(config-if-GigabitEthernet 0/2)# expert access-group acl80-guest in
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA(config)# show access-lists
expert access-list advanced sss
 10 deny 0800 FFFF 24 0A0101 FFFFFF 42
 20 deny 0800 FFFF 24 0C010102 FFFFFFFF 42
 30 permit 0806 FFFF 24
 40 permit 0800 FFFF 24

expert access-group acl80-guest in
Applied On interface GigabitEthernet 0/2
```

Ping the financial data server from a visitor PC and confirm that the ping operation fails.

Ping the public resource server from a visitor PC and confirm that the ping operation succeeds.

Ping the internal employee gateway 192.168.1.1 from a visitor PC and confirm that the ping operation fails.

Access the Internet through a visitor PC, for example, access www.baidu.com, and confirm that the home page can be opened.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
expert access-list advanced acl80-guest
 10 deny 0800 FFFF 24 0A0101 FFFFFF 42
 20 deny 0800 FFFF 24 0C010102 FFFFFFFF 42
 30 permit 0806 FFFF 24
 40 permit 0800 FFFF 24
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 expert access-group 2700 in
 ip address 11.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip address 12.1.1.1 255.255.255.0
!
```

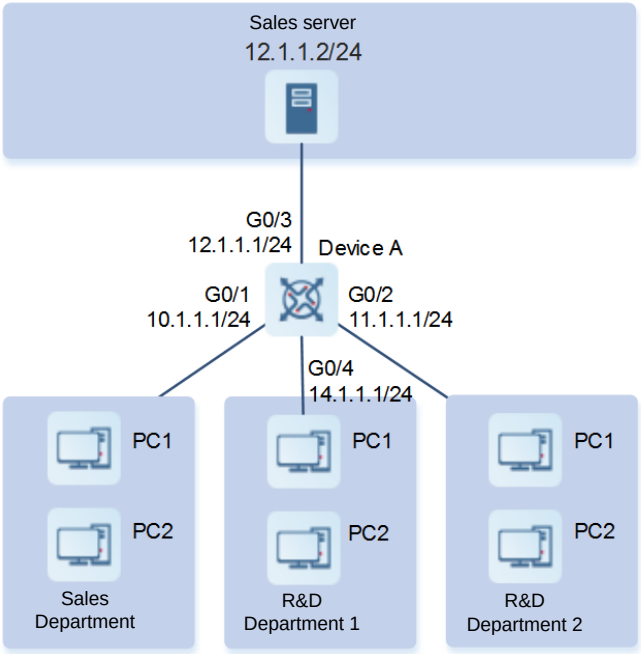
1.10.7 Configuring a Global Security ACL

1. Requirements

The global security ACL function needs to be enabled to prohibit the R&D department from accessing the sales server, but permits the sales department to access it.

2. Topology

Figure 1-9 Topology of Global Security ACL Application Scenario



3. Notes

- On device A, configure an IP extended ACL and add the rule of denying packets with the destination address 12.1.1.2/24.
- Configure the ACL as a global security ACL on device A.
- Configure the port directly connected to the sales department as an excluded port of the global security ACL on device A.

4. Procedure

(1) Configure an IP extended ACL and add access rules.

On device A, configure an IP extended ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip access-list extended ip_ext_deny_dst_sale_server
DeviceA(config-ext-nacl)# deny ip any host 12.1.1.2
DeviceA(config-ext-nacl)# exit
```

(2) Configure a global security ACL.

Configure the ACL as a global security ACL on device A.

```
DeviceA(config)# ip access-group ip_ext_deny_dst_sale_server in
```

(3) Configure an excluded port of the global security ACL.

Configure the port directly connected to the sales department as an excluded port of the global security ACL on device A.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no global access-group
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA# show access-lists
ip access-list extended ip_ext_deny_dst_sale_server
 10 deny ip any host 10.1.1.3
DeviceA# show running
……
!
ip access-group ip_ext_deny_dst_sale_server in
!
……
!
interface GigabitEthernet 0/1
 no global access-group
!
```

Ping the sales server address from a PC in the sales department, and confirm that the ping operation succeeds.

Ping the sales server address from PCs in R&D departments 1 and 2, and confirm that the ping operation fails.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
ip access-list extended ip_ext_deny_dst_sale_server
 10 deny ip any host 12.1.1.2
!
ip access-group ip_ext_deny_dst_sale_server in
!
interface GigabitEthernet 0/1
 no switchport
 no global access-group
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 11.1.1.1 255.255.255.0
!
```

```
interface GigabitEthernet 0/3
 no switchport
 ip address 12.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/4
 no switchport
 ip address 14.1.1.1 255.255.255.0
!
```

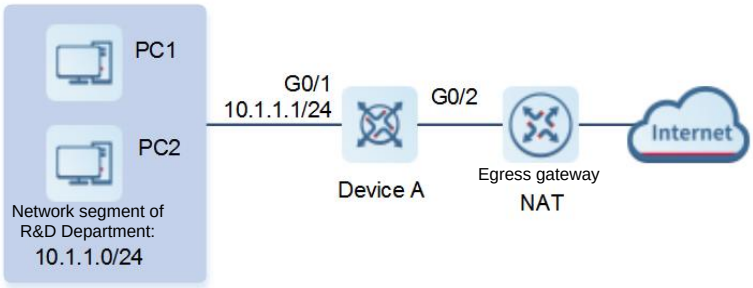
1.10.8 Configuring ACL Rules Based on Time Range

1. Requirements

ACL rules based on time range need to be configured to permit the R&D department to access the Internet only from 12:00 to 13:30 every day.

2. Topology

Figure 1-10 Topology of Time Range-based ACL Rule Application Scenario



3. Notes

- Configure a time range on device A and add the time range entry from 12:00 to 13:30 every day.
- On device A, configure an IP standard ACL and add access rules, including:
  - Permitting packets from the source IP network segment 10.1.1.0/24 and associating the rule with the time range named access-internet.
  - Denying packets from the source IP network segment 10.1.1.0/24. This rule indicates that the Internet access is rejected beyond the time range.
  - Permitting packets from network segment addresses other than the R&D network segment addresses.
- On device A, apply the ACL to the inbound direction of the port connected to the R&D department.

4. Procedure

(1) Configure a time range.

Configure a time range on device A.

```
DeviceA> enable
DeviceA# configure terminal
```

```
DeviceA(config)# time-range access-internet
DeviceA(config-time-range)# periodic daily 12:00 to 13:30
DeviceA(config-time-range)# exit
```

(2) Configure an IP standard ACL and add access rules.

On device A, configure an IP standard ACL and add access rules.

```
DeviceA(config)# ip access-list standard ip_std_internet_acl
DeviceA(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access-internet
DeviceA(config-std-nacl)# deny 10.1.1.0 0.0.0.255
DeviceA(config-std-nacl)# permit any
DeviceA(config-std-nacl)# exit
```

(3) Apply the IP standard ACL to a port.

On device A, apply the ACL to the inbound direction of the port connected the egress gateway.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip access-group ip_std_internet_acl in
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA# show time-range

time-range entry: access-internet (inactive)
  periodic Daily 12:00 to 13:30

DeviceA# show access-lists

ip access-list standard ip_std_internet_acl
 10 permit 10.1.1.0 0.0.0.255 time-range access-internet (inactive)
 20 deny 10.1.1.0 0.0.0.255
 30 permit any

DeviceA# show access-group
ip access-group ip_std_internet_acl in
Applied On interface GigabitEthernet 0/1
```

During the effective period of the time range (12:00 to 13:30), visit the home page of www.baidu.com from a PC in the R&D department, and confirm that it can be accessed.

During the ineffective period (time beyond 12:00 to 13:30), visit the home page of www.baidu.com from a PC in the R&D department, and confirm that it cannot be accessed.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
ip access-list standard ip_std_internet_acl
 10 permit 10.1.1.0 0.0.0.255 time-range access-internet
```

```
 20 deny 10.1.1.0 0.0.0.255
 30 permit any
!
time-range access-internet
 periodic daily 12:00 to 13:30
!
interface GigabitEthernet 0/1
 no switchport
 ip access-group ip_std_internet_acl in
 ip address 10.1.1.1 255.255.255.0
!
```

Contents

1 Configuring QoS 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Configuration Task Summary 7
1.3 Configuring Traffic Classification 8
1.3.1 Overview 8
1.3.2 Configuration Tasks 8
1.3.3 Configuring a Class 8
1.3.4 Configuring a Policy 9
1.3.5 Applying a Policy 10
1.3.6 Configuring a Logical Interface Group 11
1.4 Configuring Priority Mapping 12
1.4.1 Overview 12
1.4.2 Restrictions and Guidelines 12
1.4.3 Configuration Tasks 12
1.4.4 Configuring the Trust Mode 12
1.4.5 Configuring Mappings 13
1.5 Configuring the Interface Rate Limit 14
1.5.1 Overview 14
1.5.2 Restrictions and Guidelines 14
1.5.3 Procedure 14

1.6 Configuring Congestion Management 14
1.6.1 Overview 14
1.6.2 Restrictions and Guidelines 14
1.6.3 Configuration Tasks 14
1.6.4 Configuring the CoS-to-Queue Mappings 15
1.6.5 Configuring the Scheduling Policy and Round Robin Weights for Output Queues 15
1.6.6 Configuring Bandwidth for a Queue 16
1.7 Configuring Congestion Avoidance 17
1.7.1 Overview 17
1.7.2 Configuration Tasks 17
1.7.3 Enabling the WRED Function 17
1.7.4 Configuring Higher and Lower Threshold Values 18
1.7.5 Configuring the Maximum Discarding Probability 18
1.7.6 Configuring the Sampling Weight 19
1.7.7 Configuring the CoS-to-Threshold Mappings 19
1.8 Configuring the QoS Global Policy 20
1.8.1 Overview 20
1.8.2 Restrictions and Guidelines 20
1.8.3 Procedure 20
1.9 Disabling the Packet Priority Change 20
1.9.1 Overview 20
1.9.2 Procedure 20
1.10 Monitoring 21
1.11 Configuration Examples 22

1.11.1 Configuring the Interface Rate Limit and Priority Re-marking 22

1.11.2 Configuring Queue Scheduling and Congestion Avoidance 25

1 Configuring QoS

1.1 Introduction

1.1.1 Overview

Quality of service (QoS) can meet users' requirements for different applications and different levels of service quality. It allocates and schedules resources based on users' requirements and provides different levels of service quality for different packets.

On a traditional IP network, a device treats all the packets in the same way, in which the device processes packets based on their arrival time according to the queuing strategy of first in first out (FIFO), and transmits the packets to the destination on a best-effort basis. When the network bandwidth is abundant, all the packets are properly processed; when the network is congested, all the packets may be discarded.

QoS assigns a transmission priority to the packets of a type to highlight the importance of the packets. Then, the devices provide special transmission services for these packets according to forwarding policies for different priorities, congestion avoidance, and other mechanisms. With QoS, a device processes real-time and important packets preferentially, processes non-real-time and common packets with lower priorities and even discards the packets upon network congestion.

QoS enhances the network performance predictability, effectively allocates network bandwidth, and reasonably utilizes network resources.

1.1.2 Principles

1. Basic Concepts

- DiffServ model

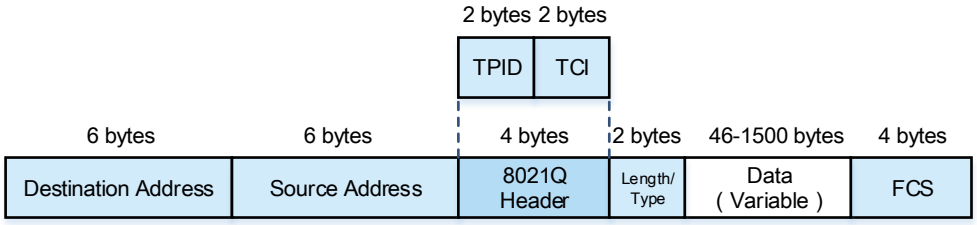
  The differentiated services (DiffServ) model classifies all packets transmitted on a network into different types. The classification information related to QoS priority marking is recorded in some fields of L2 or L3 packets, for example, the PRI field of IEEE 802.1Q frames, type of service (ToS) field of IPv4 packets, and traffic class (TC) field of IPv6 packets.

  In the network of DiffServ model, the classification information of packets can be assigned by hosts or other network devices or based on different application policies or different packet contents. A device applies the same transmission service policy to packets containing the same classification information and applies different transmission service policies to packets containing different classification information. Based on the classification information carried by packets, a device may provide different transmission priorities for different packets, reserve bandwidth for a kind of packets, discard certain packets with lower priorities, or take some other actions.

- PRI field of the IEEE 802.1q frames

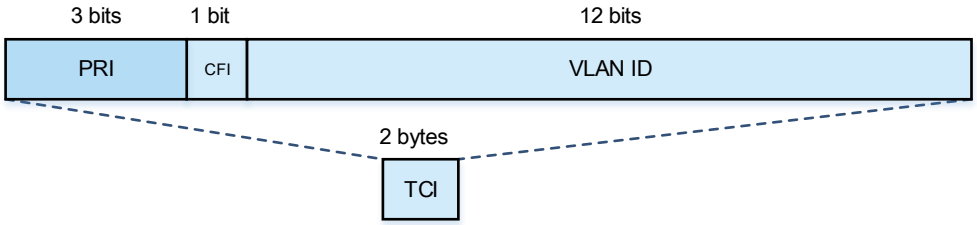
  The PRI field of IEEE 802.1Q frames (namely, the IEEE 802.1p priority) is located in the header of an L2 packet containing an IEEE 802.1Q tag header, as shown in Figure 1-1.

Figure 1-1 Format of an L2 Frame with an IEEE 802.1Q Tag Header



The 4-byte IEEE 802.1Q tag header contains the 2-byte tag protocol identifier (TPID) and 2-byte tag control information (TCI). TCI contains the 3-bit PRI field, as shown in Figure 1-2.

Figure 1-2 PRI Field of the IEEE 802.1q Frames

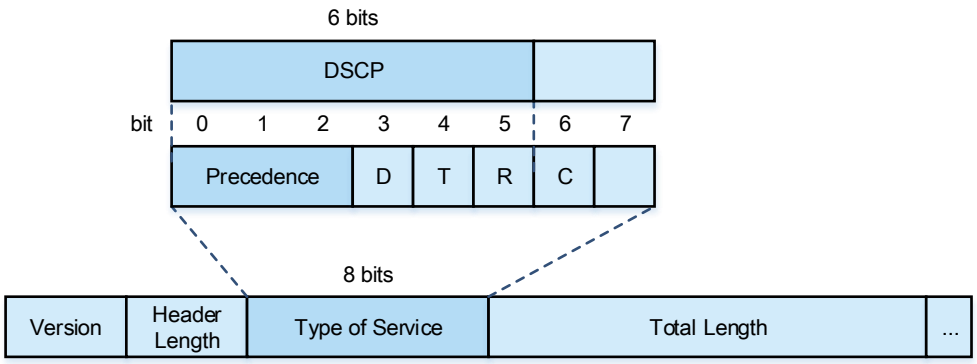


The PRI field represents eight priorities for packet transmission, and the priority values from high to low are 7, 6, ..., 1, and 0. The IEEE 802.1p priority is applicable to scenarios where L3 headers do not need to be analyzed and QoS needs to be implemented only at L2.

- ToS field of the IPv4 packets

  IPv4 packets use the ToS field in the IP header to indicate the priority of the packets, as shown in Figure 1-3.

Figure 1-3 ToS Field in the IP Header



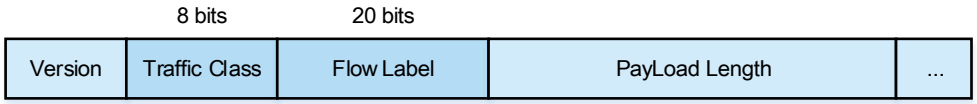
The ToS field contains eight bits, of which the first three bits are the IP PRE (precedence) field and represent eight priorities for packet transmission, with the priority values from high to low being 7, 6, ..., 1, and 0.

RFC2474 redefines the ToS field of the IP header, in which the first 6 bits (bits 0 to 5) represent the differentiated services code point (DSCP). DSCP is used to classify packets into a maximum of 64 different categories.

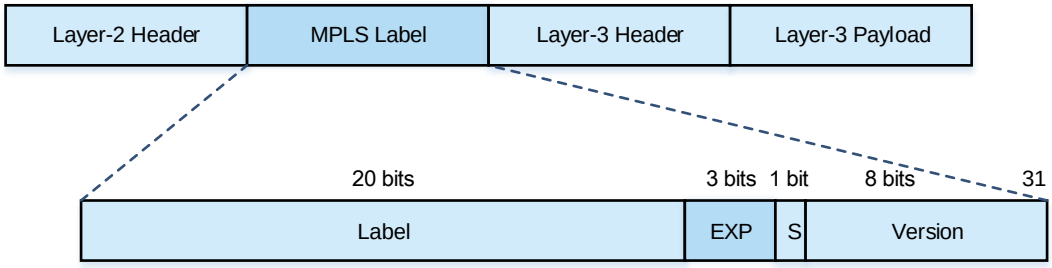
- ToS field of the IPv6 packets

  IPv6 packets use the TC field in the IPv6 header to indicate the packet priority, as shown in Figure 1-4Figure 1-4.

Figure 1-4 TC Field in the IPv6 Header



The TC field contains eight bits and provides the same function as the ToS field of IPv4 packets. The first six bits of the TC field indicate DSCP.



- CoS

  The class of service (CoS) is used to determine the packet queue number when an interface sends packets. The CoS values are 7, 6, ..., 1, and 0 from high to low.

2. Traffic Classification

Traffic classification identifies packets with certain characteristics according to rules. It is the prerequisite and basis for providing differentiated network services. Traffic classification is classified into simple traffic classification and complex traffic classification.

- Simple traffic classification

  Simple traffic classification classifies packets only based on the priorities carried in packets (for example, the PRI value of IEEE 802.1q frames, IP PRE or DSCP value of IP packets, and TC value of IPv6 packets). Simple traffic classification implements the mapping from the priority to the CoS of the device based on whether an interface is configured to trust the priority tag carried in uplink packets.

- Complex traffic classification

  Complex traffic classification classifies packets based on the priorities carried in packets or by identifying packets meeting certain characteristics according to access control list (ACL) rules.

  A QoS policy based on complex traffic classification associates the complex traffic classification with relevant traffic behaviors to form a policy, which is then applied to an interface to take effect. A QoS policy comprises three elements: class, traffic behavior, and policy.

- A class comprises the class name and class rule. A class defines the matching rules of traffic classification to classify packets.
- A traffic behavior defines the action to be taken for the classified packets, including modifying the packet priority (also known as priority re-marking) and monitoring traffic.
- A policy comprises the policy name, and the binding relationship between a class and a traffic behavior. A policy binds a specified class and a traffic behavior and is applied to one or more interfaces to take effect.

- QoS logical interface group

  You can specify a series of interfaces (aggregation ports or Ethernet interfaces) as a QoS logical interface group, and associate a policy with the logical interface group for QoS processing. For example, the rate limiting function of a traffic behavior enables the packets complying with the rate limiting conditions to share the bandwidth limited by the policy on all the interfaces in the same logical interface group.

3. Priority Mapping

Priorities are used to identify the scheduling weights or forwarding priority of packets. Different priority types are defined for different packet types: IEEE 802.1q frames use the IEEE 802.1p priority, IP packets use the IP PRE or DSCP, and so on.

After a packet enters a device interface, the packet priority is mapped to the CoS according to the trust mode configured for the interface. Table 1-1 shows the mappings between trust mode configured for an interface and the priorities.

Table 1-1 Interface Trust Mode and Priority Mapping

Interface Trust Mode	Priority Mapping
Untrusted	● No priority carried in packets is trusted. ● All packets received from an interface use the IEEE 802.1p value configured for the interface. ● The CoS values are obtained from the 802.1p-to-DSCP mapping table and DSCP-to-CoS mapping table. Packets are sent to queues based on their CoS values. ● If an IEEE 802.1Q tagged packet is sent from an egress, the packet priority is changed to the corresponding CoS value.
Trusting 802.1p	● If a packet received by an interface is an IEEE 802.1Q tagged packet, the carried IEEE 802.1p value is directly used. If a packet does not carry any tag, the IEEE 802.1p value configured for the interface is used. ● The CoS values are obtained from the 802.1p-to-DSCP mapping table and DSCP-to-CoS mapping table. Packets are sent to queues based on their CoS values. ● If an IEEE 802.1Q tagged packet is sent from an egress, the packet priority is changed to the corresponding CoS value.

Interface Trust Mode	Priority Mapping
Trusting DSCP	● If a packet received from an interface is a non-IP packet, it is processed in the same way of trusting 802.1p. If the received packet is an IP packet, the CoS value is obtained from the DSCP-to-CoS mapping table based on the DSCP value of the packet. Packets are sent to queues based on their CoS values.
Trusting IP PRE	● If a packet received from an interface is a non-IP packet, it is processed in the same way of trusting 802.1p. If the received packet is an IP packet, the CoS value is obtained from the IP PRE-to-DSCP mapping table and DSCP-to-CoS mapping table based on the IP PRE value of the packet. Packets are sent to queues based on their CoS values.

4. Traffic Policing

Traffic policing supervises the rate of the specific traffic, limits the rate within a reasonable range, and discards the traffic out of the limit or re-marks the priority. Traffic policing adopts the committed access rate (CAR) technology to control traffic. CAR uses the single-rate single-token bucket algorithm to judge whether the rate of each packet exceeds the specified traffic limit.

- Single-rate single token bucket

  The single-rate single token bucket contains two parameters: **CIR** and **CBS**.

  - Committed information rate (CIR): Indicates the rate at which a token is added to a token bucket.
  - Committed burst size (CBS): Indicates the capacity of a token bucket.

  The single-rate single token bucket adds tokens to a token bucket at a fixed rate (namely, CIR). When the number (that is, CBS) of tokens in a token bucket reaches the capacity of the token bucket, the excess tokens are discarded. When the device processes packets, it takes tokens out of the token bucket, with the number same as the size of packets (in bytes). When the number of tokens is sufficient, the packets can be forwarded. When the number of tokens is insufficient, the packets are discarded or the priorities of some packets are re-marked before forwarding.

- CAR processing

  CAR uses a token bucket to measure the packets passing through an interface, and implements the preset policing action based on the measurement results. These actions include:

  - Forwarding: Packets within the traffic limit are normally forwarded.
  - Discarding: Packets out of the traffic limit are discarded. The packets out of the total traffic limit of an interface are directly discarded.
  - Changing the priority and forwarding: The priorities of the packets out of the traffic limit are changed and then the packets are forwarded.

5. Congestion Management

When the receiving rate of packets exceeds the sending rate, congestion occurs on the sending interface. If no sufficient buffer is provided to store these packets, packet loss may occur. The congestion management mechanism determines the sending order of packets based on their local priorities. The congestion management

function controls congestion and improves the local priorities of packets for some important data. When congestion occurs, the packets of higher priorities are sent first to ensure that key services are provided in time.

Congestion management adopts the queue scheduling mechanism. The processing is as follows:

(1) After each packet undergoes the QoS processing in a device, it obtains a CoS value finally.

(2) The device allocates the packets to the corresponding sending queues according to the CoS values.

(3) The outbound interface selects the packets in a queue for sending according to various queue scheduling policies (such as SP, RR, WRR, DRR, WFQ, SP+WRR, SP+DRR, and SP+WFQ).

- SP scheduling policy

  In strict-priority (SP) scheduling, packets are scheduled strictly based on their queue priorities from high to low.

  The weakness of SP scheduling is that, when congestion occurs, if the packets in a higher priority queue exist for a long time, the packets in a lower priority queue have no opportunity of being scheduled.

- RR scheduling policy

  Round robin (RR) scheduling uses the round robin method to schedule multiple queues. Only one packet in a queue is processed each time.

- WRR scheduling policy

  The weighted round robin (WRR) scheduling solves the problem that weight cannot be set for RR scheduling. WRR scheduling also adopts the round robin method to schedule multiple queues. The number of packets in a queue processed each time is proportional to the weight of the queue. RR scheduling is equivalent to WRR scheduling with the weight 1.

  However, WRR scheduling fails to schedule the services with low delay requirements in time.

- DRR scheduling policy

  The deficit round robin (DRR) scheduling is similar to WRR scheduling, but implements scheduling based on the time slice, instead of the number of packets.

  However, DRR scheduling fails to schedule the services with low delay requirements in time.

- WFQ scheduling policy

  Weighted fair queuing (WFQ) scheduling fixes the problem that the queues using WRR scheduling have no fixed egress bandwidth. WFQ scheduling allocates an egress bandwidth to queues based on the queue weight, and different queues can have the opportunity of fair scheduling.

- SP+WRR scheduling policy

  SP scheduling is configured for one or more sending queues, and the other queues are scheduled in the WRR mode. Among SP queues, only after all the packets in an SP queue with a higher priority are sent, can the packets in an SP queue with a next higher priority be sent. Among SP and WRR queues, only after the packets in all SP queues are sent, can the packets in WRR queues be sent.

- SP+DRR scheduling policy

  SP scheduling is configured for one or more sending queues, and the other queues are scheduled in the DRR mode. Among SP queues, only after all the packets in an SP queue with a higher priority are sent, can the packets in an SP queue with a next higher priority be sent. Among SP and DRR queues, only after the packets in all SP queues are sent, can the packets in DRR queues be sent.

- SP+WFQ scheduling policy

SP scheduling is configured for one or more sending queues, and the other queues are scheduled in the WFQ mode. Among SP queues, only after all packets in an SP queue with a higher priority are sent, can the packets in an SP queue with a next higher priority be sent. Among SP and WFQ queues, only after the packets in all SP queues are sent, can the packets in WFQ queues be sent.

6. Congestion Avoidance

Congestion avoidance monitors the usage of the outbound interface queues, and eliminates the network overload by actively discarding packets and adjusting the network traffic when network congestion occurs. Congestion avoidance avoids congestion by effectively monitoring the network traffic load, forecasting the occurrence of congestion, and discarding packets. Discarding policies include tail-drop, discarding based on random early detection (RED) results, and discarding based on weighted random early detection (WRED) results.

- Tail-drop

  Traditional packet loss policies use the tail-drop method. Tail-drop is effective for all traffic and cannot distinguish service levels. When congestion occurs, data packets at the tail of a queue are discarded until the congestion is removed.

- RED and WRED

  The hosts running Transmission Control Protocol (TCP) decreases the rate of sending packets to respond to massive packet loss. After congestion is removed, the hosts increase the rate of sending packets. Tail-drop may cause TCP global synchronization. Namely, when a queue discards multiple TCP packets simultaneously, multiple TCP connections enter the congestion avoidance and slow startup state simultaneously. In this case, the tail is dropped, and the traffic is reduced and adjusted. When congestion is removed, traffic peaks appear. The process repeats constantly, the network traffic goes up and down suddenly, and the line traffic always fluctuates between the lowest traffic and the full traffic. When TCP global synchronization occurs, the connection bandwidth cannot be fully used, which causes a bandwidth waste.

  To avoid this circumstance, you can use the RED or WRED packet discarding policy. The policy provides a mechanism for discarding packets at random and avoiding TCP global synchronization. When packets of a TCP connection are discarded and the remaining packets of the TCP connection are sent at a lower rate, packets of other TCP connections are still sent at higher rates. There are always some TCP connections whose packets are sent at higher rates, which increases the utilization of line bandwidth.

  When WRED is used, you can set the lower threshold and maximum discarding probability for a queue. When the length of a queue is smaller than the lower threshold, no packets are discarded. When the queue length is between the lower threshold and higher threshold, WRED starts to discard packets randomly and sets a maximum discarding probability. A longer queue leads to a higher discarding probability. When the length of a queue is greater the higher threshold, packets are discarded at the maximum discarding probability.

  Different from RED, WRED uses priorities to distinguish discarding policies. RED is a special case of WRED. When all the CoS values of an interface are mapped to the same lower and higher thresholds, WRED becomes RED.

1.2 Configuration Task Summary

QoS configuration includes the following tasks:

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring Traffic Classification
- Configuring Priority Mapping
- Configuring the Interface Rate Limit
- Configuring Congestion Management
- Configuring Congestion Avoidance
- Configuring the QoS Global Policy
- Disabling the Packet Priority Change

1.3 Configuring Traffic Classification

1.3.1 Overview

Traffic classification uses certain rules to identify the packets with certain characteristics. You can define the binding between multiple traffic classes and traffic behaviors to form policies and apply the policies to interfaces to realize traffic classification and processing.

1.3.2 Configuration Tasks

Traffic classification configuration includes the following tasks:

(1) Configuring a Class

(2) Configuring a Policy

(3) Applying a Policy

(4) (Optional) Configuring a Logical Interface Group

1.3.3 Configuring a Class

1. Overview

This section describes how to create a class, and defines class matching rules in class configuration mode.

2. Restrictions and Guidelines

- A class name comprises a maximum of 31 characters.
- Run the **match** command to define a class matching rule.
- When setting the matching rule of a class to ACL matching, you need to create an ACL and ACL rules first.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a class and enter the class configuration mode.

class-map *class-map-name*

No class is configured by default.

(4) Define a matching rule for the class. Configure at least one of the tasks.

- Set the matching rule of the class to ACL matching.

  match access-group { *acl-number* | *acl-name* }

  Numerically indexed ACLs or named ACLs are supported.

- Set the matching rule of the class to matching the PRE priorities of IP packets.

  match ip precedence *pre-value-list*

  Multiple IP PRE values can be matched at the same time. The value range of IP PRE is from 0 to 7.

- Set the matching rule of the class to matching the DSCP priorities of IP packets.

  match ip dscp *dscp-value-list*

  Multiple DSCP values can be matched at the same time. The value range of DSCP priority is from 0 to 63.

No class matching rules are defined by default.

1.3.4 Configuring a Policy

1. Overview

This section describes how to create a policy, and bind classes and traffic behaviors in the policy configuration mode.

2. Restrictions and Guidelines

- A policy name comprises a maximum of 31 characters.
- When multiple classes are associated with the same policy, you are not advised to match the same flow with multiple classes; otherwise the traffic behavior bound to a class is performed on the flow randomly, and, when the device restarts, the traffic behavior bound to a class is also performed on the flow randomly.
- The **set** command is used to modify the priority tag of a specified packet, such as IEEE 802.1p and DSCP.
- The **police** command is used to limit the bandwidth of the specified traffic and configure the processing action on traffic beyond the limit, for example, discarding the traffic out of the limit, or modifying the CoS or DSCP value.
- The **drop** command is used to drop all the identified streams.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a policy and enter the policy configuration mode.

policy-map *policy-map-name*

No policy is configured by default.

(4) Associate a class and enter the policy class configuration mode.

class *class-map-name*

No class is associated with a policy by default.

(5) Bind the class to a traffic behavior. Configure at least one of the tasks.

- Bind the class to the traffic behavior of modifying the IEEE 802.1p and DSCP values.

  set { **cos** *new-cos* | **ip dscp** *new-dscp* }

- Bind the class to the traffic behavior of limiting the bandwidth and processing packets beyond the limit.

  police *rate-bps burst-byte* [**exceed-action** { **cos** *new-cos* | **drop** | **dscp** *new-dscp* }]

A class is not bound to any traffic behavior by default.

After the traffic behavior of discarding packets is configured, you need to delete the traffic behavior of discarding packets before configuring the above traffic behaviors.

(6) (Optional) Bind the class to the traffic behavior of discarding packets.

drop

A class is not bound to any traffic behavior by default.

This command can be configured only when a class associated with a policy is not bound to any traffic behavior. Namely, after a class associated with a policy is bound to the traffic behavior of discarding packets, you need to first delete the binding and then bind the class to other traffic behaviors.

1.3.5 Applying a Policy

1. Overview

This section describes how to apply a configured policy to a specified interface to make the policy take effect.

2. Restrictions and Guidelines

- A policy can be applied globally or to an interface.
- A policy can be applied to an L2 aggregation port or an L2 Ethernet interface. A policy can be applied to a switch virtual interface (SVI). When an L2 Ethernet interface is added to a VLAN and policies are configured for both the Ethernet interface and an SVI, the priority of the policy applied to the L2 Ethernet interface is higher than that applied to the SVI.
- If a policy is applied globally, the policy is applied to all interfaces which can be configured with policies.
- Configuring the **input** option applies a policy to the input direction of an interface.
- Configuring the **output** option applies a policy to the output direction of an interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Apply a policy. Please configure only one task.

- Apply a policy in global configuration mode.

  service-policy { **input** | **output** } *policy-map-name*

  No policy is applied globally by default.

- Apply a policy in interface configuration mode. Run the following commands in turn to apply a policy.

interface *interface-type interface-number*

service-policy { **input** | **output** } *policy-map-name*

No policy is applied to an interface by default.

1.3.6 Configuring a Logical Interface Group

1. Overview

This section describes how to associate a configured policy with a logical interface group.

2. Restrictions and Guidelines

- A maximum of 128 logical interface groups can be created.
- In global configuration mode, run the **virtual-group** command to create a logical interface group and enter the logical interface group configuration mode.
- In interface configuration mode, run the **virtual-group** command to add the interface to a specified logical interface group. If the logical interface group is not created, this command creates the logical interface group and adds the interface to the group.
- Physical interfaces or aggregation ports can be added to a logical interface group. The following types of interfaces cannot be added to a logical interface group:
  - Member interface of an aggregation port
  - VSL member interface

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a logical interface group and add interfaces to it. Please configure only one task.

- Create a logical interface group in global configuration mode and add interfaces to it. Run the following commands in turn to create a logical interface group and add interfaces to it.

  virtual-group *virtual-group-number*

  No logical interface group is defined by default.

  interface *interface-type interface-number*

  virtual-group *virtual-group-number*

  An interface is not added to any logical interface group by default.

- Create a logical interface group in interface configuration mode and add interfaces to it. Run the following commands in turn to create a logical interface group and add interfaces to it.

  interface *interface-type interface-number*

  virtual-group *virtual-group-number*

  An interface is not added to any logical interface group by default.

(4) Return to the global configuration mode.

exit

(5) Enter the logical interface group configuration mode.

virtual-group *virtual-group-number*

(6) Apply a policy to the logical interface group.

service-policy { **input** | **output** } *policy-map-name*

1.4 Configuring Priority Mapping

1.4.1 Overview

Priority mapping can be implemented based on the trust mode configured for an interface.

1.4.2 Restrictions and Guidelines

Priority mapping can be configured only on L2 and L3 Ethernet interfaces.

1.4.3 Configuration Tasks

Priority marking and mapping configuration includes the following tasks:

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Trust Mode
- Configuring Mappings

1.4.4 Configuring the Trust Mode

1. Overview

- You can set various priorities for packets according to the trust mode configured for an interface.
- Run the **mls qos trust** command to configure the trust mode for an interface.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure the trust mode for the interface. Please configure only one task.

- Configure trusting IEEE 802.1p.

  mls qos trust cos

- Configure trusting DSCP.

  mls qos trust dscp

- Configure trusting IP PRE.

  mls qos trust ip-precedence

An interface is in untrusted mode by default.

(5) (Optional) Configure the IEEE 802.1p value for the interface.

mls qos cos *cos-value*

The default IEEE 802.1p value of an interface is **0**.

1.4.5 Configuring Mappings

1. Overview

This section describes how to configure mappings, including:

- IEEE 802.1p-to-DSCP mappings.
- DSCP-to-CoS mappings.
- IP PRE-to-DSCP mappings.

2. Restrictions and Guidelines

- Run the **mls qos map cos-dscp** command to configure the mappings from IEEE 802.1p values to DSCP values.
- Run the **mls qos map dscp-cos** command to configure the mappings from DSCP values to CoS values.
- Run the **mls qos map ip-precedence-dscp** command to configure the mappings from IP PRE values to DSCP values.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure mappings. Configure at least one of the tasks.

- Configure the IEEE 802.1p-to-DSCP mappings.

  mls qos map cos-dscp *dscp-value-list*

  The IEEE 802.1p values 0 to 7 are mapped to the DSCP values 0, 8, 16, 24, 32, 40, 48, and 56 respectively by default.

- Configure the DSCP-to-CoS mappings.

  mls qos map dscp-cos *dscp-value*&<1-8> **to** *cos-value*

  DSCP values 0 to 7 are mapped to CoS 0, DSCP values 8 to 15 are mapped to CoS 1, DSCP values 16 to 23 are mapped to CoS 2, DSCP values 24 to 31 are mapped to CoS 3, DSCP values 32 to 39 are mapped to CoS 4, DSCP values 40 to 47 are mapped to CoS 5, DSCP values 48 to 55 are mapped to CoS 6, and DSCP values 56 to 63 are mapped to CoS 7 by default.

- Configure the IP PRE-to-DSCP mappings.

  mls qos map ip-precedence-dscp *dscp-value-list*

  The IP PRE values 0 to 7 are mapped to the DSCP values 0, 8, 16, 24, 32, 40, 48, and 56 respectively by default.

1.5 Configuring the Interface Rate Limit

1.5.1 Overview

This section describes how to configure traffic limit for an interface.

1.5.2 Restrictions and Guidelines

The interface type that can be configured depends on the product.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure traffic limit for the interface. Configure at least one of the tasks.

- Configure the rate limit for the traffic in the input direction of an interface.

  rate-limit input *bps burst-size*

- Configure the rate limit for the traffic in the output direction of an interface.

  rate-limit output *bps burst-size*

No traffic limit is configured for an interface by default.

1.6 Configuring Congestion Management

1.6.1 Overview

This section describes how to control congestion. The priorities of important data packets can be raised so that they are sent first when congestion occurs, thereby ensuring that key services are provided in time.

1.6.2 Restrictions and Guidelines

Congestion management can be configured only on an L2 Ethernet aggregation port or an L3 Ethernet interface.

1.6.3 Configuration Tasks

The congestion management configuration includes the following tasks:

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the CoS-to-Queue Mappings
- Configuring the Scheduling Policy and Round Robin Weights for Output Queues
- Configuring Bandwidth for a Queue

1.6.4 Configuring the CoS-to-Queue Mappings

1. Overview

This section describes how to configure the CoS-to-queue mappings so that packets can enter various output queues based on their CoS values.

2. Restrictions and Guidelines

- Run the **priority-queue cos-map** command to configure the CoS-to-queue mappings.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the CoS-to-queue mappings.

priority-queue cos-map *qid cos*&<1-8>

The CoS values 0 to 7 are mapped to the queues 1 to 8 respectively by default.

1.6.5 Configuring the Scheduling Policy and Round Robin Weights for Output Queues

1. Overview

This section describes how to configure the scheduling policy and round robin weights for output queues. The scheduling policy and round robin weight ratio for output queues are configured globally. Some products support both global configuration and interface-based configuration. Interface-based configuration has a higher priority than global configuration. The global scheduling policy works with the corresponding global round robin weight ratio, while the interface scheduling policy works with the corresponding interface round robin weight ratio. If only the global scheduling policy or interface scheduling policy is configured but no corresponding round robin weight ratio is configured, the default round robin weight ratio is used for the scheduling policy.

2. Restrictions and Guidelines

- Run the **priority-queue** command to set the scheduling policy to SP scheduling.
- Run the **mls qos scheduler sp** command to set the scheduling policy to SP scheduling for output queues.
- Run the **mls qos scheduler rr** command to set the scheduling policy to RR scheduling for output queues.
- Run the **mls qos scheduler wrr** command to set the scheduling policy to WRR scheduling based on the packet quantity for output queues.
- Run the **mls qos scheduler drr** command to set the scheduling policy to WRR scheduling based on the packet size for output queues.
- Run the **mls qos scheduler wfq** command to set the scheduling policy to WFQ scheduling for output queues.
- Run the **drr-queue bandwidth** command to configure the round robin weight for the DRR scheduling policy of output queues. A higher weight means that more packet bytes can be sent.
- Run the **wrr-queue bandwidth** command to configure the round robin weight for the WRR scheduling policy of output queues. A higher weight means longer output time. The configurable weight range depends on the product.

- Run the **wfq-queue bandwidth** command to configure the round robin weight for the WFQ scheduling policy of output queues. A higher weight means that more packet bytes can be sent. The configurable weight range depends on the product.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the scheduling policy for output queues. Please configure only one task.

- Set the scheduling policy to SP scheduling.

  priority-queue

- Configure the scheduling policy for global output queues.

  mls qos scheduler { **drr** | **rr** | **sp** | **wfq** | **wrr** }

  The default scheduling policy of global output queues is **WRR**.

- Configure the scheduling policy for interface output queues. Run the following commands in turn to configure the scheduling policy for interface output queues.

  interface *interface-type interface-number*

  mls qos scheduler { **drr** | **rr** | **sp** | **wfq** | **wrr** }

  No scheduling policy is configured on an interface by default.

(4) Configure the round robin weight for the scheduling policy of output queues. Please configure only one task.

- Configure the round robin weight for the scheduling policy of global output queues.

  { **drr-queue** | **wfq-queue** | **wrr-queue** } **bandwidth** *weight&<1-8>*

  The default round robin weight ratio of global queues is **1:1:1:1:1:1:1:1**.

- Configure the round robin weight for the scheduling policy of interface output queues. Run the following commands in turn to configure the round robin weight for the scheduling policy of interface output queues.

  interface *interface-type interface-number*

  { **drr-queue** | **wfq-queue** | **wrr-queue** } **bandwidth** *weight&<1-8>*

  The default round robin weight ratio of interface queues is **1:1:1:1:1:1:1:1**.

1.6.6 Configuring Bandwidth for a Queue

1. Overview

This section describes how to configure the minimum guaranteed bandwidth and maximum limited bandwidth for a queue.

2. Restrictions and Guidelines

- This command can be configured globally or on an interface, depending on the product.
- The configuration support is different in global configuration mode and interface configuration mode.
- Whether the **max** option can be carried in the configuration command depends on the product.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the minimum guaranteed bandwidth and maximum limited bandwidth for a queue.

qos queue *queue-id* **bandwidth** { **maximum** { *bandwidth* } | **minimum** *bandwidth* }

No minimum guaranteed bandwidth or maximum limited bandwidth is configured for a queue by default.

The value ranges of the minimum guaranteed bandwidth and maximum limited bandwidth depend on the product.

1.7 Configuring Congestion Avoidance

1.7.1 Overview

Congestion avoidance monitors the usage of queues in an outbound interface and eliminates the network overload by actively discarding packets and adjusting the network traffic in the case of network congestion.

1.7.2 Configuration Tasks

Congestion avoidance configuration includes the following tasks:

(1) Enabling the WRED Function

(2) (Optional) Configuring Higher and Lower Threshold Values

(3) (Optional) Configuring the Maximum Discarding Probability

(4) (Optional) Configuring the Sampling Weight

(5) (Optional) Configuring the CoS-to-Threshold Mappings

1.7.3 Enabling the WRED Function

1. Overview

This section describes how to configure WRED as the packet discarding policy.

2. Restrictions and Guidelines

The default packet discarding policy is tail-drop.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the WRED function.

queueing wred

The WRED function is disabled by default.

1.7.4 Configuring Higher and Lower Threshold Values

1. Overview

This section describes how to configure the higher and lower threshold values for WRED.

2. Restrictions and Guidelines

- When the packet length of a queue is smaller than the lower threshold, no packets are discarded. When the queue length is between the lower threshold and the higher threshold, WRED starts to discard packets randomly.
- Because the maximum value of the configuration range is equal to the current higher threshold, you need to pay attention to the configured higher threshold when configuring the lower threshold.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure a lower threshold value. Please configure only one task.

- Configure a lower threshold value in percentage.

  wrr-queue random-detect min-threshold *queue-id threshold*&<1-2>

  The queue value range is from 1 to 8. The value range of the lower threshold value is from 1 to the set value of the higher threshold. The default threshold value depends on the product.

The threshold value is configured in percentage by default.

1.7.5 Configuring the Maximum Discarding Probability

1. Overview

When the packet length in a queue is between the lower threshold and the higher threshold, you can configure the maximum probability for discarding packets at random.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure the maximum discarding probability.

wrr-queue random-detect probability *queue-id probability*&<1-2>

The maximum discarding probability is not configured by default.

1.7.6 Configuring the Sampling Weight

1. Overview

You can configure the sampling weight for the WRED discarding function to affect the calculation result of the average queue length.

2. Restrictions and Guidelines

- When packets are forwarded, WRED determines the discarding probability based on the average queue length of the egress queue. When the queue length is between the lower threshold and the higher threshold, WRED starts to discard packets randomly. A longer queue leads to a higher discarding probability but the probability cannot be higher than the maximum discarding probability. When the queue length is greater than the higher threshold, packets are discarded at the maximum discarding probability.
- The sampling weight indicates the weight factor of sampled data updates. A larger sampling weight indicates a longer update interval of the average queue length and a larger average queue length.
- To make the sampling weight effective, you need to first configure the WRED discarding function on an interface. Namely, the sampling weight must be configured after the higher threshold and lower threshold are configured for the WRED discarding function on an interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure the sampling weight.

wrr-queue random-detect sample-weight *queue-id weight*

No sampling weight is configured by default.

1.7.7 Configuring the CoS-to-Threshold Mappings

1. Overview

This section describes how to configure the CoS-to-threshold mappings.

2. Restrictions and Guidelines

- Multiple threshold groups can be configured for the lower threshold and maximum discarding probability.
- By configuring the mappings from CoS values and threshold groups, you can select the effective threshold group mapped to a CoS, for example, you can map CoS 0 to threshold group 1, and CoS 1 to threshold group 2.
- If the packets of CoS values 0 and 1 are all added to queue 1 for scheduling, the packets of CoS 0 are processed based on the lower threshold and maximum discarding probability in group 1, and the packets of CoS 1 are processed based on the lower threshold and maximum discarding probability in group 2.

- When all the CoS values are mapped to the same threshold group, the enabled WRED becomes RED.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure the CoS-to-threshold mappings.

wrr-queue cos-map *threshold-id cos*&<1-8>

All the CoS values are mapped to the threshold in group 1 by default.

1.8 Configuring the QoS Global Policy

1.8.1 Overview

Enabling the QoS global policy enables some QoS policies by default, for example, changing the DSCP value of L2 flows.

1.8.2 Restrictions and Guidelines

Different QoS policies may be enabled on different devices by default.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the global QoS policy.

mls qos enable

1.9 Disabling the Packet Priority Change

1.9.1 Overview

When a packet is sent out of a device, the priority of the packet is changed to the priority configured on the device. You can disable packet priority change, that is, the priority of a packet sent out of a device is the same as that when the packet is sent to the device.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable packet priority change.

mls qos remark disable

1.10 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

Running the **clear** commands may interrupt services due to loss of important information.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2 QoS Monitoring

Command	Purpose
show class-map [*class-map-name*]	Displays the traffic classification information.
show policy-map [*policy-map-name* [**class** *class-map-name*]]	Displays the QoS policy information.
show policy-map interface *interface-type interface-number*	Displays information about a policy applied to an interface.
show virtual-group [*virtual-group-number* | **summary**]	Displays information about a logical interface group.
show mls qos virtual-group [*virtual-group-number* | **policers**]	Displays information about a policy applied to a logical interface group.
show mls qos maps [**cos-dscp** | **dscp-cos** | **ip-prec-dscp**]	Displays various mappings.
show mls qos rate-limit [**interface** *interface-type interface-number*]	Displays the rate limit information of an interface.
show mls qos queueing [**interface** *interface-type interface-number*]	Displays information about the QoS queues, scheduling policies, and round robin weights.
show mls qos scheduler [**interface** *interface-type interface-number*]	Displays the scheduling policy information of an output queue.

Command	Purpose
show queueing wred [**interface** *interface-type interface-number*]	Displays the WRED configuration.
show mls qos interface *interface-type interface-number* [**policers**]	Displays the QoS information of an interface.
show qos bandwidth [**interface** *interface-type interface-number*]	Displays information about the queue bandwidth.
debug qos lib [**event** | **message**]	Debugs the QoS library.
debug qos server [**event** | **message**]	Debugs the QoS communication server.
debug qos mls	Debugs QoS user command processing.
debug qos vmsup	Debugs VMSUP configurations.

1.11 Configuration Examples

1.11.1 Configuring the Interface Rate Limit and Priority Re-marking

1. Requirements

To meet the service requirements of normal teaching, a school puts forwards the following requirements:

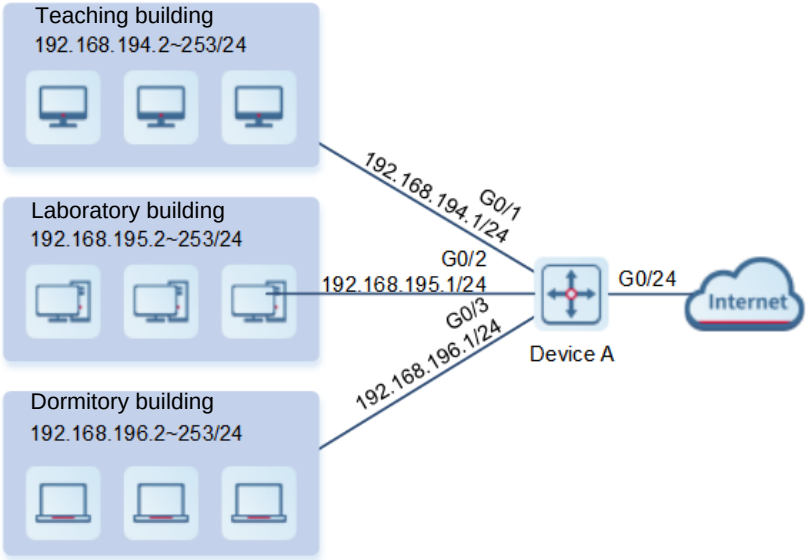
- Controlling the Internet access traffic of the school within 100 Mbps and discarding the packets out of the limit.
- Controlling the egress traffic of the dormitory building within 50 Mbps and discarding the packets out of limit.
- Controlling the rate of packets with DSCP priority 7 sent from laboratory building within 20 Mbps, and changing the DSCP priorities of the packets whose rates exceed 20 Mbps to 16.
- Controlling the egress traffic of the teaching building within 30 Mbps and discarding the packets out of limit.

Note

The school connects to the Internet through G0/24 of device A, and G0/1, G0/2, and G0/3 of device A connect to the teaching building (192.168.194.2~253/24), laboratory building (192.168.195.2~253/24), and dormitory building (192.168.196.2~253/24) respectively.

2. Topology

Figure 1-5 Application Scenario of Interface Rate Limit and Priority Re-marking



3. Notes

(1) For Internet access traffic on the outbound interface, configure the egress traffic limit on interface G0/24 of device A, and set the bandwidth limit to 102,400 kbps and burst traffic limit to 256 Kbytes per second.

(2) For the dormitory building, configure the ingress traffic limit on interface G0/3 of device A, and set the bandwidth limit to 51,200 kbps and burst traffic limit to 256 Kbytes per second.

(3) For the teaching building, configure the ingress traffic limit on interface G0/1 of device A, and set the bandwidth limit to 30,720 kbps and burst traffic limit to 256 Kbytes per second.

(4) For the laboratory building, create the class cmap_dscp7 to match DSCP priority 7, create the policy pmap_shiyan, associate cmap_dscp7 with the policy, bind the traffic behavior of changing the DSCP value of packets whose rates exceed 20 Mbps to 16, to the class, apply pmap_shiyan to interface G0/2, and configure the interface to trust DSCP.

4. Procedure

(1) Configure IP addresses for interfaces (omitted).

(2) Configure rate limits for the interfaces.

For Internet access traffic on the outbound interface, configure the egress traffic limit on interface G0/24.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/24
DeviceA(config-if-GigabitEthernet 0/24# rate-limit output 102400 256
DeviceA(config-if-GigabitEthernet 0/24)# exit
```

For the dormitory building, configure the ingress traffic limit on interface G0/3.

```
DeviceA(config)# interface gigabitethernet 0/3
DeviceA(config-if-GigabitEthernet 0/3# rate-limit input 51200 256
```

```
DeviceA(config-if-GigabitEthernet 0/3)# exit
```

For the teaching building, configure the ingress traffic limit on interface G0/1.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1# rate-limit input 30720 256
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

(3) Configure traffic classification.

For the laboratory building, configure a class, traffic behavior, and policy.

```
DeviceA(config)# class-map cmap_dscp7
DeviceA(config-cmap)# match ip dscp 7
DeviceA(config-cmap)# exit
DeviceA(config)# policy-map pmap_shiyan
DeviceA(config-pmap)# class cmap_dscp7
DeviceA(config-pmap-c)# police 20480 128 exceed-action dscp 16
DeviceA(config-pmap-c)# exit
DeviceA(config-pmap)# exit
```

Apply the policy to an interface and configure the interface to trust DSCP.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2# service-policy input pmap_shiyan
DeviceA(config-if-GigabitEthernet 0/2)# mls qos trust dscp
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

5. Verification

Check whether the interface rate limits are successfully configured.

```
DeviceA# show mls qos rate-limit
Interface: GigabitEthernet 0/1
  rate limit input Kbps = 30720 burst = 256
Interface: GigabitEthernet 0/3
  rate limit input Kbps = 51200 burst = 256
Interface: GigabitEthernet 0/24
  rate limit output Kbps = 102400 burst = 256
```

Check whether the class is successfully created.

```
DeviceA# show class-map cmap_dscp7

 Class Map cmap_dscp7
   Match ip dscp 7
```

Check whether the policy is successfully created.

```
DeviceA# show policy-map pmap_shiyan

 Policy Map pmap_shiyan
    Class cmap_dscp7
      police 20480 128 exceed-action dscp 16
```

Check whether the policy is applied to the interface successfully.

```
DeviceA# show mls qos interface gigabitethernet 0/2
```

```
Interface: GigabitEthernet 0/2
Ratelimit input:
Ratelimit output:
Attached input  policy-map: pmap_shiyan
Attached output policy-map:
Default trust: dscp
Default cos: 0
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
class-map cmap_dscp7
 match ip dscp 7
!
policy-map pmap_shiyan
 class cmap_dscp7
  police 20480 128 exceed-action dscp 16
!
interface GigabitEthernet 0/1
 ip add 192.168.194.1 255.255.255.0
 rate-limit input 30720 256
!
interface GigabitEthernet 0/2
 ip add 192.168.195.1 255.255.255.0
 service-policy input pmap_shiyan
 mls qos trust dscp
!
interface GigabitEthernet 0/3
 ip add 192.168.196.1 255.255.255.0
 rate-limit input 51200 256
!
interface GigabitEthernet 0/24
 rate-limit output 102400 256
!
```

1.11.2 Configuring Queue Scheduling and Congestion Avoidance

1. Requirements

Priority re-marking and queue scheduling need to be configured to meet the following requirements:

- When the R&D department and market department access the servers, the priorities of the server packets are as follows: packets destined for the mail server > packets destined for the file server > packets destined for the salary query server.
- No matter when the HR management department accesses the Internet or servers, device A processes the corresponding packets with the highest priority.
- Network congestion often occurs during operation of device A. WRR queue scheduling must be used to

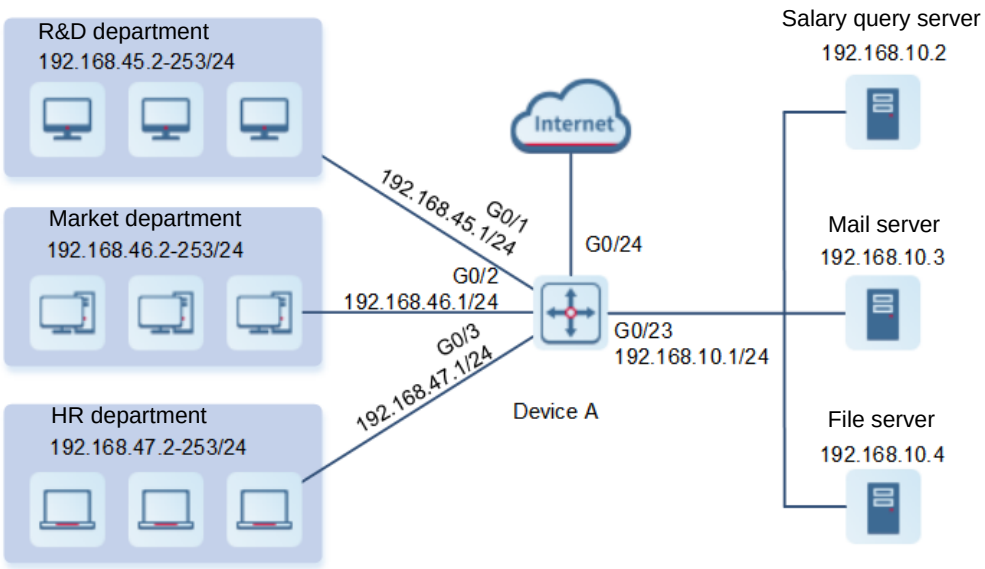
schedule IP packets from the R&D and market departments to access the mail database, file database, and salary query database based on the ratio of 6:2:1.

Note

The R&D department (192.168.45.2~253/24), market department (192.168.46.2~253/24), and HR department (192.168.47.2~253/24) are connected to interfaces G0/1, G0/2, and G0/3 of device A respectively; the salary query server (192.168.10.2/24), mail server (192.168.10.3/24), and file server (192.168.10.4/24) are connected to interface G0/23 of device A.

2. Topology

Figure 1-6 Application Scenario of Queue Scheduling and Congestion Avoidance



3. Notes

(1) On device A, create ACLs to filter packets used for accessing servers, create classes, and associate the classes with these ACLs.

(2) Create policies to associate with the classes and specify the IEEE 802.1p values for the packets accessing various servers in the policies: Set the IEEE 802.1p value to 4 for the packets accessing the mail server, to 3 for the packets accessing the file server, and to 2 for the packets accessing the salary query server. Apply the policies to the inbound interfaces connected to the R&D and market departments and configure the interfaces to trust IEEE 802.1p.

(3) Assign the highest priority 7 to the IEEE 802.1p value of the interface connected to the HR department, to ensure that packets from the HR department are sent with the highest priority.

(4) Set the scheduling policy to WRR for output queues and set the round robin weight to 1:1:1:2:6:1:1:0 for the queues. This means that SP scheduling is used for packets of the HR department, and the packets for accessing the mail database, file database, and salary query database from the R&D and market departments are scheduled based on the ratio of 6:2:1.

(5) Enable the WRED function.

(6) Set the lower thresholds to 10 and 20 for queue 2 of interface G0/2.

(7) Set the higher thresholds to 60 and 90 for queue 2 of interface G0/2.

(8) Set the maximum discarding probabilities to 60 and 80 for queue 2 of interface G0/2.

4. Procedure

(1) On device A, configure ACLs to filter packets used for accessing the servers and add ACL rules.

Configure the ACL for matching packets used for accessing the salary query server as well as ACL rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip access-list extended salary
DeviceA(config-ext-nacl)# permit ip any host 192.168.10.2
DeviceA(config-ext-nacl)# exit
```

Configure the ACL for matching packets used for accessing the mail server as well as ACL rules.

```
DeviceA(config)# ip access-list extended mail
DeviceA(config-ext-nacl)# permit ip any host 192.168.10.3
DeviceA(config-ext-nacl)# exit
```

Configure the ACL for matching packets used for accessing the file server as well as ACL rules.

```
DeviceA(config)# ip access-list extended file
DeviceA(config-ext-nacl)# permit ip any host 192.168.10.4
DeviceA(config-ext-nacl)# exit
```

(2) Configure classes on device A.

Configure a class named salary and associate it with the ACL for matching packets used for accessing the salary query server.

```
DeviceA(config)# class-map salary
DeviceA(config-cmap)# match access-group salary
DeviceA(config-cmap)# exit
```

Configure a class named mail and associate it with the ACL for matching packets used for accessing the mail server.

```
DeviceA(config)# class-map mail
DeviceA(config-cmap)# match access-group mail
DeviceA(config-cmap)# exit
```

Configure a class named file and associate it with the ACL for matching packets used for accessing the file server.

```
DeviceA(config)# class-map file
DeviceA(config-cmap)# match access-group file
DeviceA(config-cmap)# exit
```

(3) Configure policies on device A.

Configure a policy and associate the class named class with a traffic behavior in the policy.

```
DeviceA(config)# policy-map toserver
DeviceA(config-pmap)# class salary
DeviceA(config-pmap-c)# set cos 2
```

```
DeviceA(config-pmap-c)# exit
```

Configure a policy and associate the class named salary with a traffic behavior in the policy.

```
DeviceA(config-pmap)# class mail
DeviceA(config-pmap-c)# set cos 4
DeviceA(config-pmap-c)# exit
```

Configure a policy and associate the class named mail with a traffic behavior in the policy.

```
DeviceA(config-pmap)# class file
DeviceA(config-pmap-c)# set cos 3
DeviceA(config-pmap-c)# exit
DeviceA(config-cmap)# exit
```

(4) Apply policies on device A.

Apply a policy to the interface of device A that is connected to the R&D department.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# service-policy input toserver
DeviceA(config-if-GigabitEthernet 0/1)# mls qos trust cos
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Apply a policy to the interface of device A that is connected to the market department.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# service-policy input toserver
DeviceA(config-if-GigabitEthernet 0/2)# mls qos trust cos
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

(5) On device A, configure the 802.1p field for an interface.

Configure the highest priority for the 802.1p field for the interface connected to the HR department.

```
DeviceA(config)# interface gigabitethernet 0/3
DeviceA(config-if-GigabitEthernet 0/3)# mls qos cos 7
DeviceA(config-if-GigabitEthernet 0/3)# exit
```

(6) On device A, configure a scheduling policy for output queues.

Set the scheduling policy to WRR for output queues.

```
DeviceA(config)# wrr-queue bandwidth 1 1 1 2 6 1 1 0
DeviceA(config)# mls qos scheduler wrr
```

(7) Configure congestion avoidance on device A.

Enable the WRED function.

```
DeviceA(config)# queueing wred
```

Configure the higher and lower threshold values.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# wrr-queue random-detect min-threshold
2 10 20
DeviceA(config-if-GigabitEthernet 0/2)# wrr-queue random-detect probability 2
60 80
```

Configure the CoS-to-threshold mappings.

```
DeviceA(config-if-GigabitEthernet 0/2)# wrr-queue cos-map 2 0 1 2 3
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

5. Verification

Check whether ACLs are successfully created.

```
DeviceA# show access-lists

ip access-list extended file
 10 permit ip any host 192.168.10.4

ip access-list extended mail
 10 permit ip any host 192.168.10.3

ip access-list extended salary
 10 permit ip any host 192.168.10.2
```

Check whether the classes are successfully associated with the ACLs.

```
DeviceA# show class-map

 Class Map salary
   Match access-group salary
 Class Map mail
   Match access-group mail
 Class Map file
   Match access-group file
```

Check whether policies are successfully created, and whether the classes and traffic behaviors are successfully bound.

```
DeviceA# show policy-map

 Policy Map toserver
    Class mail
      set cos 4
    Class file
      set cos 3
    Class salary
      set cos 2
```

Check whether a policy is successfully applied to interface GigabitEthernet 0/1.

```
DeviceA# show mls qos interface gigabitethernet 0/1
Interface: GigabitEthernet 0/1
Ratelimit input:
Ratelimit output:
Attached input  policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
```

Check whether a policy is successfully applied to interface GigabitEthernet 0/2.

```
DeviceA# show mls qos interface gigabitethernet 0/2
Interface: GigabitEthernet 0/2
Ratelimit input:
Ratelimit output:
Attached input  policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
```

Check whether a policy is successfully applied to interface GigabitEthernet 0/3.

```
DeviceA# show mls qos interface gigabitethernet 0/3
Interface: GigabitEthernet 0/3
Ratelimit input:
Ratelimit output:
Attached input  policy-map:
Attached output policy-map:
Default trust: none
Default cos: 7
```

Check whether the 802.1p value is successfully configured for the interface and whether the scheduling policy and the round robin weight are successfully configured.

```
DeviceA# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8

wrr bandwidth weights:
qid weights
--- -------
1   1
2   1
3   1
4   2
5   6
6   1
7   1
8   0
```

```
drr bandwidth weights:
qid weights
--- -------
1   1
2   1
3   1
4   1
5   1
6   1
7   1
8   1

wfq bandwidth weights:
qid weights
--- -------
1   1
2   1
3   1
4   1
5   1
6   1
7   1
8   1
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
wrr-queue bandwidth 1 1 1 2 6 1 1 0
queueing wred
wrr-queue cos-map 2 0 1 2 3
!
class-map salary
 match access-group salary
class-map mail
 match access-group mail
class-map file
 match access-group file
!
policy-map toserver
 class salary
  set cos 2
 class mail
  set cos 4
 class file
  set cos 3
```

```
!
interface GigabitEthernet 0/1
 ip add 192.168.45.1 255.255.255.0
 service-policy input toserver
 mls qos trust cos
!
interface GigabitEthernet 0/2
 ip add 192.168.46.1 255.255.255.0
 wrr-queue random-detect min-threshold 2 10 20
 service-policy input toserver
 mls qos trust cos
!
interface GigabitEthernet 0/3
 ip add 192.168.47.1 255.255.255.0
 mls qos cos 7
!
```

Contents

1 Configuring MMU 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Configuration Task Summary 4
1.3 Configuring Buffer Adjustment 4
1.3.1 Overview 4
1.3.2 Restrictions and Guidelines 4
1.3.3 Configuration Tasks 4
1.3.4 Configuring the Global Buffer Mode 5
1.3.5 Configuring a Guaranteed Buffer for a Queue 5
1.3.6 Configuring a Shared Buffer for a Queue 6
1.3.7 Configuring a Flow Control Threshold for a Port 6
1.4 Configuring Status Monitoring 7
1.4.1 Overview 7
1.4.2 Restrictions and Guidelines 7
1.4.3 Procedure 7
1.5 Configuring Exception Detection 7
1.5.1 Overview 7
1.5.2 Configuration Tasks 7
1.5.3 Configuring an Alarm Threshold for the Buffer Utilization of a Port Group or Slice 7
1.5.4 Configuring an Alarm Threshold for the Buffer Utilization of a Queue 8

1.5.5 Configuring a Buffer Utilization Alarm Threshold for a Port.....8

1.6 Monitoring 9

1.7 Configuration Examples.....10

1.7.1 Configuring the Application of a Large Buffer Based on Egress Queues 10

1 Configuring MMU

1.1 Introduction

1.1.1 Overview

The memory management unit (MMU) is a technology for allocating the chip buffers reasonably. This technology makes devices better deal with all kinds of burst flows.

Flows are not always steady and various burst flows exist in the network. When the network flow is steady and the bandwidth is sufficient, all the data flows are processed properly. When burst flows exist in the network, data flows may be discarded even if the average flow rate does not exceed the bandwidth. Data packets are stored in the buffers of a device before being forwarded. Normally, data packets in the buffers will be forwarded in microseconds. When a burst flow arises, if the instantaneous rate of the burst flow is out of the processing capacity of the device, the data packets that cannot be processed in time are piled up in the buffers and packet loss takes place once the buffers are insufficient. In this case, the MMU technology can used to reasonably configure buffers and allocate different buffer sizes to services, with a view to optimizing the network.

1.1.2 Principles

1. Basic Concepts

- Port group

  All the ports that physically belong to the same switching chip and the same core (some chips are multi-core chips) are called a port group. All devices implement buffer management in port groups.

- Buffer slice

  The buffer of a port group may be divided into multiple buffer blocks, and each buffer block is called a buffer slice. Slice is the minimum unit for independent buffer management. Each buffer slice is managed independently, and a port queue may use one or more buffer slices.

- Guaranteed buffer

  A guaranteed buffer is also called an exclusive buffer. This part of buffer is distributed based on each port queue. The guaranteed buffer of a queue can be used by this queue only. A fixed number of guaranteed buffers are allocated to each queue by default. This part of buffer enables a queue to normally forward packets at the line rate under the stable flow.

- Shared buffer

  In the total buffer of a port group, the remaining part obtained after the guaranteed buffer of each port queue is deducted is the total shared buffer. The shared buffer is available to all the queues. A shared buffer threshold can be set for each queue. This threshold restricts the maximum number of shared buffers that can be used by a queue. When the sum of shared buffers configured for queues in a port group exceeds the total shared buffers of the port group, the "first-come first-served" buffer occupancy mechanism is adopted.

- Service pool

In addition to the guaranteed buffer, each port queue can use shared buffers. The shared buffers are uniformly stored in the service pool for management. One buffer slice may have multiple service pools. After using its own guaranteed buffer, each queue can request a shared buffer from the service pool within the shared buffer threshold, and the mechanism of "first-request, first-served" is adopted for the service pool. One queue can use the shared buffer of only one service pool according to the mapping configuration.

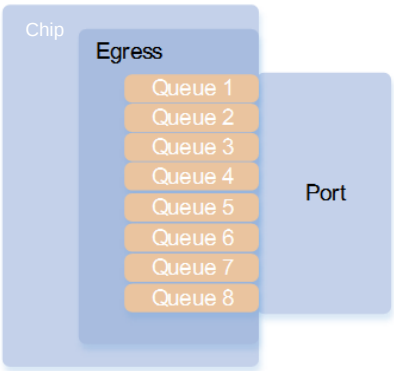
- Priority group (PG)

  PG is the abbreviation of priority group. For the sake of better and flexible buffer management, a chip offers eight PG objects in the ingress direction to implement independent buffer management. Packets are configured with different priorities (for example, 0 to 7) and can be mapped to different PG objects or one PG so that different buffer allocation schemes are provided for packets with different priorities.

- Egress queues

  Egress queues of a port are classified into unicast queues and multicast queues (the number of queues depends on the product). Logically, a switching chip is divided into the ingress direction and egress direction. The egress queues are in the egress direction of a switching chip. Before packets are sent out of a device, they need to be queued at the egress queues, as shown in Figure 1-1.

Figure 1-1 Egress Queues



Currently, there are three types of egress queue models:

- There are eight unicast queues and eight multicast queues at the egress. The known unicast packets enter the unicast queues, and all the other packets enter the multicast queues.
- There are eight unicast queues and four multicast queues at the egress. The known unicast packets enter the unicast queues, and all the other packets enter the multicast queues.
- There are only eight queues at the egress, with unicast and multicast queues not differentiated. The queues are managed as unicast queues in the device.

- Global multicast queue

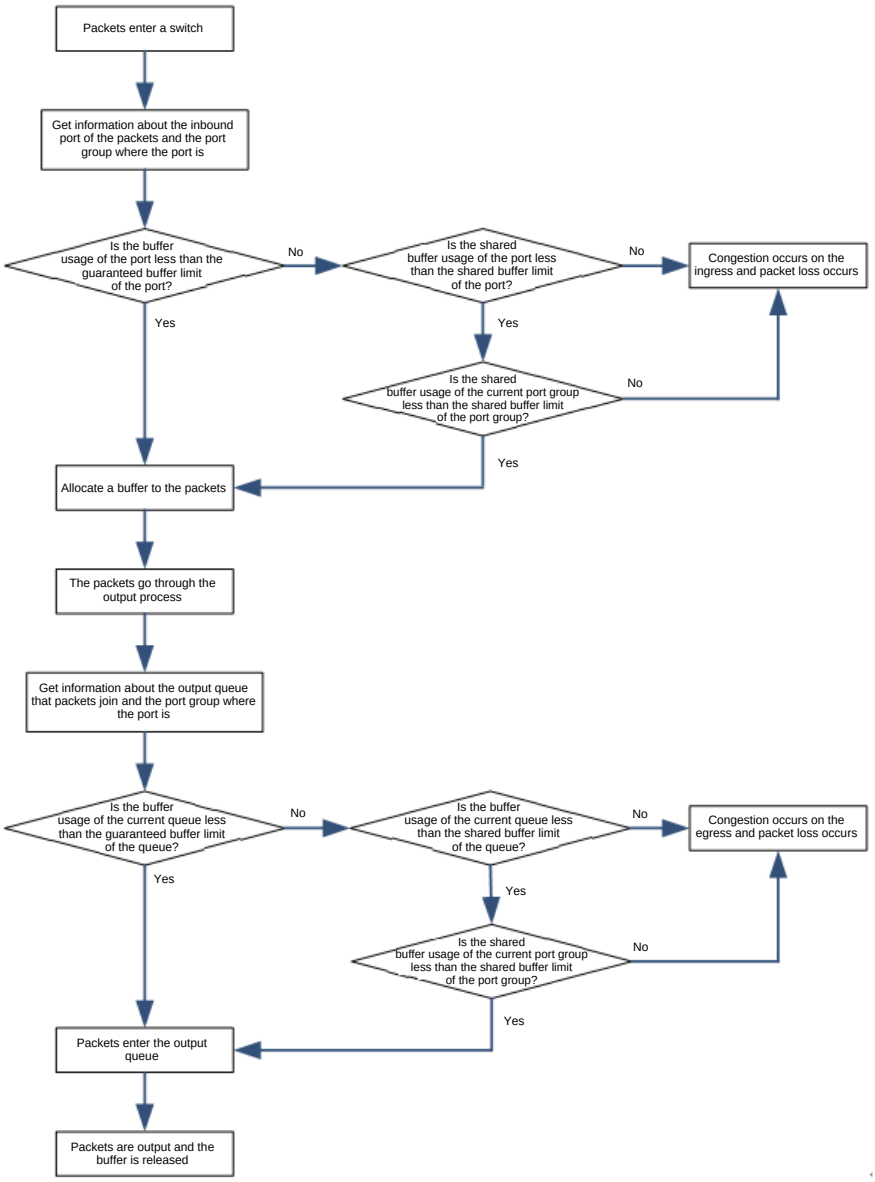
  A global multicast queue refers to the multicast queue shared by all the ports in a port group, and is different from the multicast queue owned by a single physical port.

2. Buffer Adjustment

Users can adjust the buffer allocation of a chip so that the queue of each service has a different buffer size available, services are treated differently, and services of different priorities are provided.

In terms of hardware, the buffer is managed in the input direction and output direction. Figure 1-2 shows the processing mechanism.

Figure 1-2 Buffer Processing Mechanism



During buffer management, the buffer size is adjusted to the maximum value in the input direction to prevent packet loss in the input direction, and packet loss takes place in the output direction. Therefore, buffer adjustment is not allowed in the input direction, and a CLI command is available for buffer adjustment in the output direction only, including the guaranteed buffer and shared buffer of queues. Buffer adjustment allocates different buffer sizes to queues based on the guaranteed buffer threshold and shared buffer threshold configured for the queues.

3. Status Monitoring

Status monitoring monitors the buffer usage and the queue packet forwarding and discarding by using statistical methods, with a view to providing data support for network optimization and reasonable buffer configuration.

Status monitoring adopts the polling mode to periodically read, from a chip, the buffer usage information and information about packets forwarded/discarded by queues, and analyzes the information so as to display the device operating status.

- Monitoring buffer occupancy in the egress direction

  The information about the guaranteed buffer, shared buffer, and service pool buffer occupancy of queues in the egress direction is regularly collected. The data can be displayed via a CLI command, in MIB mode, or other methods.

- Monitoring packet forwarding and discarding of the egress queues

  The information about the quantities and bytes of packets forwarded and discarded by queues in the egress direction is regularly collected, and the forwarding rate is also calculated. The data can be displayed via a CLI command, in MIB mode, or other methods.

- Sampling interval for status monitoring data

  Status monitoring data is sampled at a fixed interval, which can be configured based on user requirements.

4. Exception Detection

The exception detection function monitors the packet forwarding and discarding of each queue, and displays alarms when the buffer occupancy exceeds the threshold or queue packets are lost.

Exception detection adopts the polling mode to periodically read device buffer occupancy information and the number of packets forwarded by queues, and displays alarms through system logs based on the current configuration. When the buffer utilization of a queue exceeds the threshold, a system log alarm is printed to alert users.

1.2 Configuration Task Summary

MMU configuration includes the following tasks:

- Configuring Buffer Adjustment
- Configuring Status Monitoring
- Configuring Exception Detection

1.3 Configuring Buffer Adjustment

1.3.1 Overview

The buffer adjustment function aims to adjust the objects (such as queues) managed based on chip buffers.

1.3.2 Restrictions and Guidelines

- Configuration on an interface can be made on a physical port only.
- You are advised to configure buffer adjustment when there is no traffic on the device; otherwise the configuration may cause temporary interruption of service traffic.

1.3.3 Configuration Tasks

Buffer adjustment configuration includes the following tasks:

- Configuring the Global Buffer Mode

- Configuring a Guaranteed Buffer for a Queue
- Configuring a Shared Buffer for a Queue
- Configuring a Flow Control Threshold for a Port

1.3.4 Configuring the Global Buffer Mode

1. Overview

This section describes how to configure the global buffer mode. After configuration, the device configures the default thresholds according to the mode.

2. Restrictions and Guidelines

N/A

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the global buffer mode.

mmu buffer-mode { **burst-enhance** | **flowctrl-enhance** | **normal** | **qos-enhance** }

The default global buffer mode is **flowctrl-enhance**.

1.3.5 Configuring a Guaranteed Buffer for a Queue

1. Overview

This section describes how to configure a guaranteed buffer for a queue so that the queue uses this part of buffer exclusively.

2. Restrictions and Guidelines

- The **set** *value* parameter indicates the value of guaranteed buffer for a queue. Range: 1-50, unit: cell.
- The *queue-id* &<1-8> parameter means that up to 8 queue numbers can be configured. Whether this parameter is supported and the value range of this parameter depend on the actual product version.
- The configuration is displayed when the **show running-config** command is executed even if the default value is used.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a guaranteed buffer for queues.

mmu queue-guarantee { **output unicast** } [*queue-id*&<1-n>] **set** *value*

No guaranteed buffer is configured for a queue by default.

1.3.6 Configuring a Shared Buffer for a Queue

1. Overview

This section describes how to configure a shared buffer for a queue so as to control the size of the shared buffer that can be used by the queue.

2. Restrictions and Guidelines

- The *queue-id*&<1-8> parameter means that up to 8 queue numbers can be configured.
- The configuration is displayed when the **show running-config** command is executed even if the default value is used.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a shared buffer for queues.

mmu queue-threshold { **output unicast** } [*queue-id*&<1-n>] **set** *threshold* |

No shared buffer is configured for a queue by default.

1.3.7 Configuring a Flow Control Threshold for a Port

1. Overview

This section describes how to configure a flow control threshold for a port and adjust the flow control threshold of the ingress.

2. Restrictions and Guidelines

- The configuration takes effect only when flow control/priority-based flow control (PFC) is enabled on a port.
- The configuration is displayed when the **show running-config** command is executed even if the default value is used.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a flow control threshold for the port.

mmu fc-threshold set *threshold*

No flow control threshold is configured for a port by default.

1.4 Configuring Status Monitoring

1.4.1 Overview

This section describes how to collect statistics on and monitor the buffer usage and queue packet forwarding and discarding so as to provide guidance for buffer adjustment configuration.

1.4.2 Restrictions and Guidelines

- The configuration is displayed when the **show running-config** command is executed even if the default value is used.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a sampling period.

mmu sample-period set *period*

No monitoring data sampling period is configured by default.

1.5 Configuring Exception Detection

1.5.1 Overview

The exception detection function is used to analyze the data about device buffer and forwarding status, and generate an alarm when an exception occurs.

1.5.2 Configuration Tasks

Exception detection configuration includes the following tasks:

- Configuring an Alarm Threshold for the Buffer Utilization of a Port Group or Slice
- Configuring an Alarm Threshold for the Buffer Utilization of a Queue
- Configuring a Buffer Utilization Alarm Threshold for a Port

1.5.3 Configuring an Alarm Threshold for the Buffer Utilization of a Port Group or Slice

1. Overview

When the buffer utilization of a port group or slice exceeds the configured value, a system log alarm is printed.

2. Restrictions and Guidelines

- To prevent frequent log refreshing, the alarm logs of the same port group or slice are printed once in 30s at

most. The maximum printing interval depends on the configured sampling period.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a buffer utilization alarm threshold.

mmu usage-warn-limit set *threshold*

The default buffer utilization alarm threshold is **0**, indicating that no alarm is reported.

This configuration takes effect for all the port groups or slices.

1.5.4 Configuring an Alarm Threshold for the Buffer Utilization of a Queue

1. Overview

When the buffer utilization of a queue exceeds the configured value, a system log alarm is printed.

2. Restrictions and Guidelines

- The **set** *threshold* parameter indicates the alarm threshold for the buffer utilization of a queue. Range: 1-100, unit: percentage.
- The *queue-id* &<1-8> parameter means that up to 8 queue numbers can be configured. Whether this parameter is supported and the value range of this parameter depend on the actual product version.
- To prevent frequent log refreshing, the alarm logs of the same queue are printed once in 30s at most. The maximum printing interval depends on the configured sampling period.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a buffer utilization alarm threshold for a queue.

mmu usage-warn-limit { **unicast** } [*queue-id*&<1-n>] **set** *threshold*

The default buffer utilization alarm threshold is **0**, indicating that no alarm is reported.

1.5.5 Configuring a Buffer Utilization Alarm Threshold for a Port

1. Overview

When the buffer utilization of all the queues on a port exceeds the configured value, a system log alarm is printed.

2. Restrictions and Guidelines

- To prevent frequent log refreshing, the alarm logs of the same port are printed once in 30s at most. The

maximum printing interval depends on the configured sampling period.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configuring a buffer utilization alarm threshold for a port.

mmu usage-warn-limit set *threshold*

The default buffer utilization alarm threshold is **0**, indicating that no alarm is reported.

1.6 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

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

Table 1-1 MMU Monitoring

Command	Purpose
show [**mmu**] **queue-counter** [**interface** [*interface-type interface-number*]]	Displays the packet statistics of a queue.
Show queue-buffer [**interface** [*interface-type interface-number*]]	Displays the buffer utilization information of a queue.
show mmu buffer-mode	Displays the current buffer mode.
clear queue-counter [{ **interface** *interface-type interface-number*]	Clears the packet statistics of a queue.
clear [**mmu**] **queue-buffer peaked** [{ **interface** *interface-type interface-number*]	Clears the historical buffer utilization peak values of a queue.
clear queue-buffer usage-warn-count	Clears the count of buffer alarms of a queue.

1.7 Configuration Examples

1.7.1 Configuring the Application of a Large Buffer Based on Egress Queues

1. Requirements

An enterprise needs a buffer large enough for the net disk service to avoid packet loss occurring in the service flow.

As shown in the following figure, device A is connected to 5 clients and 35 service servers, and 15 service servers are virtualized as 15 front-end servers.

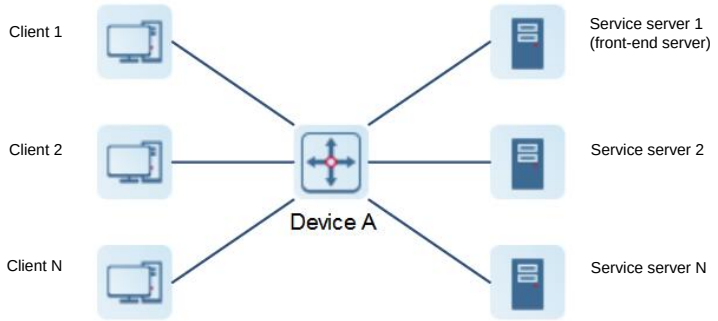
The main service flow is as follows:

- A client sends a request packet to a front-end server.
- The front-end server sends the received request packet to a service server.
- After receiving the request packet, the service server sends a response packet to the front-end server.
- After receiving the response packet, the front-end server sends it to the client.
- The client receives the response packet, indicating that a session is created successfully.
- A many-to-one flow transmission mode exists in this service model:
- The request flows of multiple clients are sent to one front-end server.
- The request flows of multiple front-end servers are sent to one service server.
- The response flows of multiple service servers are sent to one front-end server.
- The response flows of multiple front-end servers are sent to one client.

These flows are basically transmitted through device A, which can easily lead to network congestion. Such a problem can be fixed by configuring a large buffer on the device.

2. Topology

Figure 1-3 Application Scenario of a Large Buffer Based on Egress Queues



3. Notes

- On all the service ports (namely, the ports connecting to clients and servers), set the shared buffer to 100% for the queues where the service is.
- On all the service ports, set the guaranteed buffer to the minimum size for queues not in use.
- On all the ports not in use, set the guaranteed buffer to the minimum size for all the queues.

4. Procedure

(1) Configure a shared buffer.

On device A, set a shared buffer for queues on all the service ports.

```
DeviceA> enabel
DeviceA# configure terminal
DeviceA(config)# interface range gigabitethernet 0/1-40
DeviceA(config-if-range)# mmu queue-threshold output unicast 1 set 100
DeviceA(config-if-range)# exit
```

(2) Configure a guaranteed buffer.

On device A, set a guaranteed buffer for queues on all the service ports.

```
DeviceA# configure terminal
DeviceA(config)# interface range gigabitethernet 0/1-40
DeviceA(config-if-range)# mmu queue-guarantee output unicast 2 3 4 5 6 7 8 set
1
DeviceA(config-if-range)# exit
```

On device A, set a guaranteed buffer for queues on all the ports not in use.

```
DeviceA(config)# interface range gigabitethernet 0/41-48
DeviceA(config-if-range)# mmu queue-guarantee output unicast set 1
DeviceA(config-if-range)# exit
```

5. Verification

On device A, verify that the command configuration for interface GigabitEthernet 0/1 is correct.

```
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# show this

Building configuration...
!
 mmu queue-threshold output unicast 1 set 100
 mmu queue-guarantee output unicast 2 set 1
 mmu queue-guarantee output unicast 3 set 1
 mmu queue-guarantee output unicast 4 set 1
 mmu queue-guarantee output unicast 5 set 1
 mmu queue-guarantee output unicast 6 set 1
 mmu queue-guarantee output unicast 7 set 1
 mmu queue-guarantee output unicast 8 set 1
```

6. Configuration Files

Device A configuration file

The configuration of interface GigabitEthernet 0/1 to interface GigabitEthernet 0/40 is exactly the same, and therefore only the configuration of GigabitEthernet 0/1 is provided below. The configuration of interface GigabitEthernet 0/41 to interface GigabitEthernet 0/48 is exactly the same, and therefore only the configuration of GigabitEthernet 0/41 is provided below.

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 mmu queue-threshold output unicast 1 set 100
 mmu queue-guarantee output unicast 2 set 1
 mmu queue-guarantee output unicast 3 set 1
 mmu queue-guarantee output unicast 4 set 1
 mmu queue-guarantee output unicast 5 set 1
 mmu queue-guarantee output unicast 6 set 1
 mmu queue-guarantee output unicast 7 set 1
 mmu queue-guarantee output unicast 8 set 1
!
interface gigabitEthernet 0/41
 mmu queue-guarantee output unicast 1 set 1
 mmu queue-guarantee output unicast 2 set 1
 mmu queue-guarantee output unicast 3 set 1
 mmu queue-guarantee output unicast 4 set 1
 mmu queue-guarantee output unicast 5 set 1
 mmu queue-guarantee output unicast 6 set 1
 mmu queue-guarantee output unicast 7 set 1
 mmu queue-guarantee output unicast 8 set 1
!
```

Security Configuration

1. AAA Configuration
2. RADIUS Configuration
3. TACACS Configuration
4. IEEE 802.1X Configuration
5. Web Authentication Configuration
6. SCC Configuration
7. Password Policy Configuration
8. SSH Configuration
9. Global IP-MAC Address Binding Configuration
10. Port Security Configuration
11. IP Source Guard Configuration
12. IPv6 Source Guard Configuration
13. SAVI Configuration
14. ARP Check Configuration
15. DAI Configuration
16. ARP Spoofing Prevention Configuration
17. CPP Configuration
18. NFPP Configuration
19. Storm Control Configuration
20. uRPF Configuration
21. DoS Protection Configuration
22. Security Log Auditing Configuration

Contents

1 Configuring AAA 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Restrictions and Guidelines 6
1.3 Configuration Task Summary 7
1.4 Configuring an AAA Server Group 7
1.4.1 Overview 7
1.4.2 Restrictions and Guidelines 7
1.4.3 Procedure 8
1.5 Configuring Basic Features of AAA Authentication 8
1.5.1 Overview 8
1.5.2 Restrictions and Guidelines 8
1.5.3 Configuration Tasks 9
1.5.4 Configuring Login Authentication 9
1.5.5 Configuring Enable Authentication 10
1.5.6 Configuring IEEE 802.1X Authentication 11
1.5.7 Configuring 2nd-Generation Web Authentication 11
1.5.8 Configuring FTP Authentication 13
1.6 Configuring a General Authentication Method 13
1.6.1 Overview 13
1.6.2 Restrictions and Guidelines 13
1.6.3 Procedure 13

1.7 Configuring AAA Authentication Logging 14

1.7.1 Overview 14

1.7.2 Procedure 14

1.8 Configuring Basic Features of AAA Authorization 14

1.8.1 Overview 14

1.8.2 Restrictions and Guidelines 14

1.8.3 Procedure 15

1.9 Configuring the Function of Caching Command Authorization Results 16

1.9.1 Overview 16

1.9.2 Restrictions and Guidelines 16

1.9.3 Procedure 16

1.10 Configuring the Default Role for AAA Users 16

1.10.1 Overview 16

1.10.2 Restrictions and Guidelines 16

1.10.3 Procedure 16

1.11 Configuring the Function of Allowing Users to Log in to the Slave Device 17

1.11.1 Overview 17

1.11.2 Restrictions and Guidelines 17

1.11.3 Procedure 17

1.12 Configuring Basic Features of AAA Accounting 17

1.12.1 Overview 17

1.12.2 Restrictions and Guidelines 17

1.12.3 Procedure 17

1.13 Configuring a Policy for User Accounting Start Failures 18

1.13.1 Overview 18

1.13.2 Procedure 18

1.14 Configuring Domain-Based AAA Services 19

1.14.1 Overview 19

1.14.2 Restrictions and Guidelines 19

1.14.3 Procedure 19

1.15 Monitoring 20

1.16 Configuration Examples 20

1.16.1 Configuring Local Login Authentication and Local EXEC Authorization 20

1.16.2 Configuring Enable Authentication 22

1.16.3 Configuring Command Authorization 24

1.16.4 Configuring Network Authorization 24

1.16.5 Configuring an AAA Server Group 25

1.16.6 Configuring Domain-based AAA Services 27

1.17 Common Errors 29

1 Configuring AAA

1.1 Introduction

1.1.1 Overview

Authentication, authorization and accounting (AAA) is a network security management mechanism, which provides basic authentication, authorization, and accounting (billing) services for users who access networks. The content of AAA is described as follows:

- Authentication service: Identifies users before they access networks to check whether the users have access permissions.
- Authorization service: Classifies user permissions to grants different access permissions to users.
- Accounting service: Records users' usage of network resources. The statistical data can be used for analysis and billing.

AAA boasts strong flexibility and controllability, scalability, standardized authentication, and supports multiple backup systems. Compared with simple access control functions provided by devices such as local username authentication and line password-based authentication, AAA provides a higher level of security protection and therefore becomes the overriding access control method.

1.1.2 Principles

1. Basic Concepts

- Security method

  A security method refers to the method used to implement authentication, authorization, and accounting services. Security methods can be classified into AAA authentication methods, AAA authorization methods, and AAA accounting methods by service type.

  Based on the service provider, service methods can be further classified into service methods providing no security management, service methods providing security management through a local device, and service methods providing security management through a remote server. For details, see 1.1.2 3. AAA Authentication, 1.1.2 4. AAA Authorization, and 1.1.2 5. AAA Accounting.

- Method list

  Method lists are classified into authentication method lists, authorization method lists, and accounting method lists based on the AAA service type. Each method list provides multiple security methods for this type of AAA service, to ensure that alternative methods are available if one method is unavailable.

  A method list contains one or more security methods. The sequence for the methods to take effect is subject to the sequence of security methods defined in the list, that is, a method defined earlier takes effect earlier. If a method fails to respond during AAA service provision, a device switches to the next method until all methods in the method list are tried. If a method returns a failure or all methods fail to respond, the process stops and the device cannot provide the security service for users.

Notice

A device tries the next method only when no response is received from the previous method. For example, if a method denies user access during identity authentication, the identity authentication process ends and the device does not switch to other identity authentication methods.

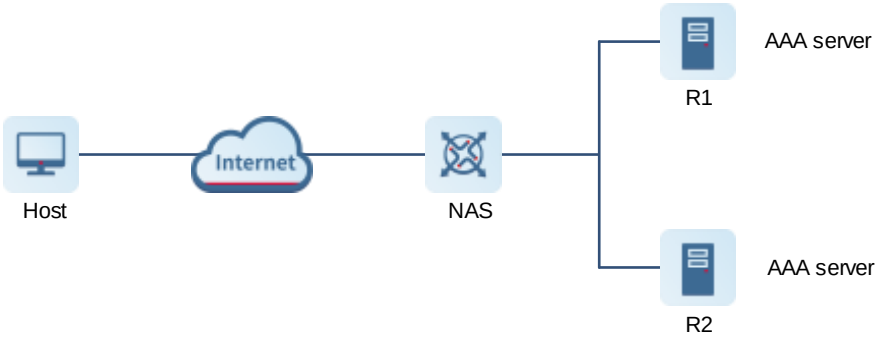
- AAA server group

  An AAA server is a device that provides remote AAA security services for users.

  An AAA server group is a collection of one or more AAA servers of the same type and provides security services for users as a security method.

2. AAA Basic Architecture

Figure 1-1 **Topology of a Typical AAA Network**



As shown in Figure 1-1, a typical AAA network consists of hosts (users), a network access server (NAS), and an AAA server (remote server). AAA uses the client/server (C/S) structure. A host sends an AAA request to the NAS as a client. After receiving the request, the NAS requests the AAA security services from the AAA server as a client and provides network access permissions for the host based on the returned result.

- Main roles

  Host: A host is a device that requests network access permissions and usually refers to a user.

  NAS: A NAS responds to hosts' network access requests and manages the hosts by using security methods provided by an AAA server.

  AAA server: An AAA server provides security methods for the NAS.

- Brief process of typical AAA services

  a Configure a method list and enable the AAA security services on the NAS. The method list provides three security methods: R1 server, R2 server, and local username database (with the effective sequence from left to right). Host-related identity information has been configured in the three methods.

  b After a host connects to the NAS through a network, the NAS provides the AAA security services for the host by using a method in the method list. According to the sequence that the methods take effect, the NAS requests the security services from R1 first.

  c If R1 responds to the NAS successfully, the NAS provides network access permissions for the host based on security information provided by R1. If R1 does not respond, the NAS switches the security

method and requests the security services from R2, and so on until all methods in the method list are used up.

Instruction

An AAA server can use a Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) server. Unless otherwise specified in this document, the RADIUS server is used as the AAA server. For details about TACACS+, see "Configuring TACACS" in the *Security Configuration Guide*.

3. AAA Authentication

AAA authentication checks information (username and password) about a user who requests the access service, to determine whether the user has the network access permission.

- AAA authentication methods

  AAA authentication methods are classified into authentication exemption, local authentication, and remote server group authentication based on the method provider.

  - Authentication exemption

    User legitimacy is not checked. This method is used only when users are very trustworthy. You are not advised to use this method.

  - Local authentication

    Local authentication uses the database on the NAS to manage user information (such as usernames, passwords, and attributes) and identify user identities.

  - Remote server group authentication

    This authentication method uses the user database on the remote server to manage user data and identify user identities. It can achieve multi-device centralized authentication with large capacity and high reliability. A remote server group supports RADIUS servers and TACACS+ servers.

- AAA authentication types

  AAA authentication is classified into login authentication, enable authentication, IEEE 802.1X authentication, 2nd-generation Web authentication, and File Transfer Protocol (FTP) authentication based on the user access mode.

  - Login authentication

    This authentication verifies user identities when the users log in to the command line interface (CLI) of the NAS through Secure Shell (SSH), telnet, or FTP.

  - Enable authentication

    After users log in to the NAS CLI, this authentication verifies the users' identity information before their CLI execution permissions are elevated, that is, users are authenticated before they enter the privileged EXEC mode.

  - IEEE 802.1X authentication

    This authentication is used to verify identities of IEEE 802.1X access users.

  - 2nd-generation Web authentication

This authentication uses a 2nd-generation portal server to verify the identities of users who access networks.

- FTP authentication

  FTP authentication is especially used for FTP users. If no FTP authentication method is configured, login authentication is used to authenticate FTP users.

- General authentication method

  You can specify a general authentication method for IEEE 802.1X authentication and 2nd-generation Web authentication. If no authentication method is configured for 2nd-generation Web authentication and IEEE 802.1X authentication or the configured methods fail to respond, the configured general authentication method takes effect as an alternative method.

4. AAA Authorization

AAA authorization is used to manage services available to users and control network access permissions of access users. After the AAA authorization service is enabled, users can use only permitted services and are granted permissions in their permitted scopes.

- AAA authorization methods

  AAA authorization methods are classified into direct authorization, local authentication, and remote server group authentication based on the method provider.

  - Direct authorization

    Direct authorization provides default permissions that the access device allows users to use. It is used only when users are very trustworthy.

  - Local authorization

    Configure attribute authorization for local users on the NAS, which completes the authorization.

  - Remote server group authorization

    Configure user attribute authorization on the remote server. The NAS completes authorization by means of a remote server group. When all servers in a remote server group fail, you can configure local authorization or direct authorization as an alternative method.

- AAA authorization types

  AAA authorization is classified into EXEC authorization, command authorization, config-commands authorization, console authorization, and network authorization based on the permission type.

  - EXEC authorization

    EXEC authorization grants different privilege levels (0–15) to users when the users log in to the NAS CLI.

    EXEC authorization is usually used in conjunction with login authentication. After login authentication and EXEC authorization are configured on the same line, if a user passes login authentication but fails in EXEC authorization, the user cannot open the CLI.

  - Command authorization

    Command authorization grants authorization to commands after users log in to the NAS CLI.

    When a user enters a command and attempts to run it, AAA sends the command to the security server. If the security server allows this command, the command is executed. Otherwise, the command is not executed and a command execution denial message is displayed.

- Config-commands authorization

  This authorization grants authorization to commands in configuration modes (including the global configuration mode and sub-modes).

- Console authorization

  This authorization grants authorization to commands to be executed by users who log in through the console.

  The system can differentiate users who log in through the console from those who log in through other terminals. You can enable or disable command authorization for users who log in through the console. If command authorization is disabled for users who log in through the console, the command authorization method list that has been applied to the console line no longer takes effect.

- Network authorization

  Network authorization grants available network services to users, such as traffic, bandwidth, and timeout services.

  Network authorization is based on authentication. Network authorization is available only for authenticated users. The RADIUS or TACACS+ server grants permissions to authenticated users by returning a series of attributes.

5. AAA Accounting

AAA accounting is used to record users' usage of network resources to implement billing, auditing, and tracking functions.

The accounting service starts accounting after a user passes authentication and records the user's network access activities. It stops accounting when the user logs out, and generates a network resource access report for the user.

- AAA accounting methods

  AAA accounting methods are classified into no accounting, local accounting, and remote server group accounting based on the method provider.

  - No accounting

    Accounting is not performed on users.

  - Local accounting

    Local accounting is completed by the NAS, which collects statistics on and limits the number of local user connections. The fee calculation function is unavailable.

  - Remote server group accounting

    Accounting is performed by a remote server. You can configure local accounting as an alternative method to avoid an accounting failure occurring when all servers in a remote server group fail.

- AAA accounting types

  AAA accounting can be classified into EXEC accounting, command accounting, and network accounting based on the accounting content.

  - EXEC accounting

    Accounting is both performed when users log in to and log out of the NAS CLI.

  - Command accounting

Command accounting is used to record commands run by a user after the user logs in to the NAS CLI from a terminal.

- Network accounting

  Network accounting is used to record information about sessions of users who access the network (such as IEEE 802.1X users and 2nd-generation Web-authenticated users).

6. Multi-Domain AAA

In multi-domain AAA, users are assigned to different domains and independent security methods are defined for each domain so that users in different domains use different security methods.

In a multi-domain environment, you can configure a separate AAA method list for each domain on the NAS. Therefore, users with the same attribute can be assigned to the same domain for the ease of management.

- Basic principles of AAA service based on domain names

  a A user submits identity authentication information to the NAS.

  b The NAS resolves the domain name in the identity authentication information.

  c The NAS checks whether the domain name is defined. If no, the NAS refuses to provide security services. If yes, the NAS makes further judgment.

  d If no method list is defined for the domain name, the NAS refuses to provide security services. If a method list is defined, the NAS provides security services.

- Username forms

  A username can be expressed in four forms. In the usernames below, "domain-name" indicates a domain name.

  - userid@domain-name
  - domain-name\userid
  - userid.domain-name
  - userid

  In the preceding username forms, the username form (userid) with no domain name uses the default domain name (**default**).

- Domain name matching

  If the username of an authenticated user carries domain information but the domain is not configured on the NAS, the NAS cannot provide AAA services for the user.

  Exact match is adopted to match domain names carried in usernames with those configured on the NAS. For example, if domain.com and domain.com.cn are configured on the NAS and a username is expressed in the form of aaa@domain.com, the NAS determines that the user belongs to domain.com rather than domain.com.cn.

1.2 Restrictions and Guidelines

- Before configuring any AAA function, run the **aaa new-model** command to enable the AAA security services. Otherwise, no command can be configured.
- AAA authentication, authorization, and accounting are three independent processes. You can use only the authentication service without authorization or accounting.

- The basic methodology and process of configuring the AAA authentication, authorization, or accounting services are as follows:
  - a Enable AAA security services.
  - b Determine the required AAA security service type based on the scenario.
  - c Configure an AAA method list for the security service type.
  - d In a corresponding mode, apply an AAA method list to make it take effect (methods do not need to be applied for some security services. For details, see specific configuration tasks).

    If this step is not configured, methods configured in step C do not take effect but the default method is used.
- Configure user information before configuring security methods.
  - To use the remote server group method, configure user data on remote servers. For details about how to configure user data, see the operation instructions of the remote servers.
  - To use the local method, configure local user data on the local device. For details about local users, see "Configuring Basic Management" in the *Basic Configuration Manual*.

1.3 Configuration Task Summary

AAA configuration includes the following tasks:

(1) (Optional) Configuring an AAA Server Group

(2) Configuring AAA Authentication

- Configuring Basic Features of AAA Authentication
- (Optional) Configuring a General Authentication Method
- (Optional) Configuring AAA Authentication Logging

(3) (Optional) Configuring AAA Authorization

- Configuring Basic Features of AAA Authorization
- (Optional) Configuring the Function of Caching Command Authorization Results
- (Optional) Configuring the Default Role for AAA Users

(4) (Optional) Configuring AAA Accounting

- Configuring Basic Features of AAA Accounting
- (Optional) Configuring a Policy for User Accounting Start Failures

(5) (Optional) Configuring Domain-Based AAA Services

1.4 Configuring an AAA Server Group

1.4.1 Overview

AAA usually uses the remote server group method to provide AAA services for users. This method provides more flexible and rich security services than the local method.

1.4.2 Restrictions and Guidelines

- One or more servers can be added to each server group.

- Both RADIUS and TACACS+ support server group configuration. The configuration procedure below uses RADIUS as an example. For details about a TACACS+ server group, see "Configuring TACACS" in the *Security Configuration Guide*.
- When configuring the authentication, authorization, and accounting method lists, you can specify different server groups for them.
- In a custom server group, only servers in the default server group can be specified and applied.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an AAA custom server group.

aaa group server radius *group-name*

No server group is configured by default.

The name of a server group cannot be set to a predefined keyword "radius" or "tacacs+".

(4) Add an AAA server group member.

server { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port* | **acct-port** *acct-port*] *

No AAA server group member is added to a server group by default.

(5) (Optional) Specify a VRF instance for the AAA server group.

ip vrf forwarding *vrf-name*

No VRF instance is specified for an AAA server group by default.

When a server group in a specified VRF instance is used, the source IP address used by the device to communicate with a remote server needs to be acquired from the VRF instance. If you run the **ip radius source-interface** command to specify the source interface of request packets, the IP address obtained from this source interface is prior to that acquired from the VRF instance.

(6) Configure the MGMT interface for the AAA server group.

ip oob [**via mgmt** *mgmt-number*]

An AAA server group uses MGMT 0 by default.

1.5 Configuring Basic Features of AAA Authentication

1.5.1 Overview

AAA authentication is used to verify user identities. After AAA authentication is configured, users can access network resources only after passing the authentication specified in security methods in the method list.

1.5.2 Restrictions and Guidelines

- After AAA authentication is configured, if no authentication method is configured and the default authentication method does not exist, users can log in through the console without authentication but other types of access users need to pass local authentication.

- If multiple methods are defined in the method list, when a method fails to respond, the device switches to the next method. The execution sequence of methods is the sequence of methods configured in the method list. If a method responds and returns a failure, the device does not switch to the next method.
- If you have passed login authentication (except the authentication exemption method) when logging in to the CLI, the device records the username, and then uses the username for authentication when Enable authentication is performed. You do not need to enter the username again but the entered password must match the username. If login authentication fails or the authentication exemption method is used when you log in to the CLI, the username will not be recorded, and you need to enter the username for authentication in the further Enable authentication.
- The authentication exemption method allows any user to access network resources without authentication. You are not advised to use this method. Only in some special cases (all access users are trustworthy and no network failure caused by authentication system problems is allowed), this method can be used as an alternative method when the device receives no response in the remote server group authentication and local authentication.

1.5.3 Configuration Tasks

Configure basic features of AAA authentication. Select at least one of the following tasks to configure.

- Configuring Login Authentication
- Configuring Enable Authentication
- Configuring IEEE 802.1X Authentication
- Configuring 2nd-Generation Web Authentication
- Configuring FTP Authentication

1.5.4 Configuring Login Authentication

1. Overview

After login authentication is configured, access users who log in through SSH, telnet, or FTP need to be authenticated before accessing network resources.

2. Restrictions and Guidelines

A configured login authentication method must be applied to a line that needs login authentication. Otherwise, the method does not take effect.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Configure a login authentication method list.

aaa authentication login { **default** | *list-name* } *method*&<1-4>

No login authentication method list is configured by default.

(5) (Optional) Configure the maximum number of consecutive failed login attempts.

aaa local authentication attempts *max-attempts*

The default maximum number of consecutive failed login attempts is **3**.

(6) (Optional) Configure the user lockout duration.

aaa local authentication lockout-time *lockout-time*

After the number of login attempts of a user exceeds the configured number of consecutive failed login attempts, the user is locked out for 15 minutes by default.

(7) Enter the configuration mode of a specified line.

line { **console** | **vty** } *first-line* [*last−line*]

(8) Apply the login authentication method list to the line.

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

The default login authentication method list applied to a line is the default method list.

1.5.5 Configuring Enable Authentication

1. Overview

After Enable authentication is configured and a user logs in to the NAS CLI through a terminal, the user must be authenticated before running the **enable** command to enter the privileged EXEC mode.

1. Restrictions and Guidelines

After an Enable authentication method list is configured, the Enable authentication function takes effect automatically.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Configure an Enable authentication method list.

aaa authentication enable default *method*&<1-4>

No Enable authentication method list is configured by default.

1.5.6 Configuring IEEE 802.1X Authentication

1. Overview

After IEEE 802.1X authentication is configured on an interface, users connected to the interface must be authenticated before accessing network resources.

2. Restrictions and Guidelines

For details about IEEE 802.1X configuration, see "Configuring IEEE 802.1X" in the *Security Configuration Guide*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Configure the address and key of a RADIUS server.

radius-server host { *ipv4-address* | *ipv6-address* } [**key** [**0** | **7**] *text-string*]

The address and key of a RADIUS server are not configured by default.

(5) Configure an IEEE 802.1X authentication method list.

aaa authentication dot1x { **default** | *list-name* } *method*&<1-4>

No IEEE 802.1X authentication method list is configured by default.

(6) Apply the IEEE 802.1X authentication method list.

dot1x authentication { **default** | *list-name* }

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Enable IEEE 802.1X authentication on the interface.

dot1x port-control auto

IEEE 802.1X authentication is disabled on a port by default.

1.5.7 Configuring 2nd-Generation Web Authentication

1. Overview

After 2nd-generation Web authentication is configured, identity authentication needs to be performed by a 2nd-generation portal server.

2. Restrictions and Guidelines

- If a local account is used for authentication, you can run the **aaa local user allow public account** command to enable the function of allowing multiple clients to share one account.
- For details about Web authentication configuration, see "Configuring Web Authentication" in the *Security*

Configuration Guide.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Configure the address and key of a RADIUS server.

radius-server host { *ipv4-address* | *ipv6-address* } [**key** [**0** | **7**] *text-string*]

The address and key of a RADIUS server are not configured by default.

(5) Configure the communication key between the NAS and the portal server.

web-auth portal key *key-string*

No key is configured for the communication between the device and the authentication server by default.

(6) Configure a 2nd-generation Web authentication method list.

aaa authentication web-auth { **default** | *list-name* } *method*&<1-4>

(7) Enter the 2nd-generation Web authentication template configuration mode.

web-auth template eportalv2

(8) Configure parameters for the 2nd-generation Web authentication template.

a Configure an authentication method list for the template.

authentication *method-list*

The default authentication method list is used by a template by default.

b Configure an IP address for the portal server used for Web authentication.

ip [*ip-address* | **oob** | **vrf** *name*]

No IP address and VRF instance are specified for the Web authentication server by default.

c Configure the authentication page of the portal server used for Web authentication.

url *url-string*

No page address of the authentication server is configured by default.

(9) Return to the global configuration mode.

exit

(10) Enter the interface configuration mode.

interface *interface-type interface-number*

(11) Enable 2nd-generation Web authentication on the interface.

web-auth enable eportalv2

2nd-generation Web authentication is disabled on a port by default.

1.5.8 Configuring FTP Authentication

1. Overview

After FTP authentication is configured, FTP users need to pass FTP authentication upon login.

2. Restrictions and Guidelines

If the AAA FTP security service is enabled on a device, users must perform FTP authentication through AAA.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Enable the FTP server function.

ftp-server enable

The FTP server function is disabled by default.

(5) Configure an FTP authentication method list.

aaa authentication ftp { **default** | *list-name* } *method*&<1-4>

No FTP authentication method list is configured by default.

(6) Configure FTP to use AAA accounts for login authentication.

ftp-server authentication { **default** | *list-name* }

FTP does not support login authentication on AAA accounts by default.

1.6 Configuring a General Authentication Method

1.6.1 Overview

A general authentication method can be used as an alternative method of 2nd-generation Web authentication and IEEE 802.1X authentication. If no authentication method is configured for 2nd-generation Web authentication or IEEE 802.1X authentication or the configured method fails to respond, the general authentication method takes effect as an alternative method.

1.6.2 Restrictions and Guidelines

If both IEEE 802.1X authentication and 2nd-generation Web authentication are configured on the device, you can configure a general method for them together.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Configure a general authentication method list.

aaa authentication general { **default** | *list-name* } *method*&<1-4>

No general authentication method is configured by default.

1.7 Configuring AAA Authentication Logging

1.7.1 Overview

The device generates logs when an AAA user passes authentication. If a large number of users go online concurrently, the device generates considerable logs, which may degrade the device performance or cause frequent screen refreshing. In this case, you can disable the logging function or restrict the logging rate.

1.7.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure AAA authentication logging. Please configure only one task.

- Disable AAA authentication logging.

  no aaa log enable

  AAA authentication logging is enabled by default.

- Configure the rate of AAA authentication logging.

  aaa log rate-limit *rate-limit*

  Five AAA authentication logs are printed per second by default.

1.8 Configuring Basic Features of AAA Authorization

1.8.1 Overview

AAA authorization is used to manage services available to users and control network use permissions of access users. After the basic features of AAA authorization are enabled, users can use only the permitted services and are granted permissions in their permitted scopes.

1.8.2 Restrictions and Guidelines

- EXEC authorization is usually used together with login authentication. Authentication and authorization can use different methods and different servers, and the authentication and authorization results of the same user may be different. If a user passes login authentication but fails in EXEC authorization, the user cannot open

the CLI.

- When configuring command authorization, specify the command level, which is used as the default level of commands. For example, if a command is visible to users above level 14, the default level of the command is 14.
- EXEC authorization and command authorization need to be applied to a line so that they take effect.
- Command authorization is unavailable when role-based access control (RBAC) is enabled. For details about RBAC, see "Configuring RBAC" in the *Basic Configuration Guide*.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an AAA authorization method. Configure at least one of the tasks.

- Configure an EXEC authorization method list to authorize permitted users to open the CLI.

  aaa authorization exec { **default** | *list-name* } *method*&<1-4>

  No EXEC authorization method list is configured by default.

- Configure a network authorization method list to authorize permitted users to access network services.

  aaa authorization network { **default** | *list-name* } *method*&<1-4>

  No network authorization method list is configured by default.

- Grant authorization to all commands in configuration modes.

  aaa authorization config-commands

  The authorization for commands in configuration modes is disabled by default.

- Enable command authorization for users who log in through the console. You can enable command authorization for users who log in through the console and users who log in through other terminals separately.

  aaa authorization console

  Command authorization is disabled for users who log in through the console by default.

(4) (Optional) Enter the configuration mode of a specified line.

line { **console** | **vty** } *first-line* [*last−line*]

(5) (Optional) Apply the authorization method to the specific line. Please configure only one task.

- Apply the EXEC authorization method to the specific line.

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

  EXEC authorization is disabled by default.

- Apply the command authorization method to the specific line.

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

  The command authorization function is disabled by default.

1.9 Configuring the Function of Caching Command Authorization Results

1.9.1 Overview

After this function is configured, the device locally caches command authorization results returned by the AAA server. For subsequent commands with the level same as the cached authorized commands, command authorization can be performed based on the locally cached results.

1.9.2 Restrictions and Guidelines

Authorization results in the local cache apply only to the current session and commands of the current level. The authorization of other sessions or commands of other levels are performed by the remote server and local authorization can be performed only after their results are cached locally.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the function of caching command authorization results.

aaa command-author cache

The function of caching command authorization results is disabled by default.

1.10 Configuring the Default Role for AAA Users

1.10.1 Overview

This function is used to configure the global user role. If no role is configured for an authorized user, the role is used by default. Different roles have different levels of command execution permissions on the device. The global user role **network-operator** is used by default. This role has the permission to run commands of the lowest level on the device.

1.10.2 Restrictions and Guidelines

- Run the **aaa new-model** and **role enable** commands before configuring this function.
- For details about user roles, see "Configuring RBAC" in the *Basic Configuration Guide*.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the default role for AAA authorized users.

aaa user-role default { *priv-level* | *role-name* | **network-admin** | **network-operator** }

The default role of AAA authorized users is **network-operator**.

1.11 Configuring Basic Features of AAA Accounting

1.11.1 Overview

AAA accounting is used to record users' usage of network resources, login and logout processes, and command execution information.

1.11.2 Restrictions and Guidelines

- EXEC accounting is performed only on users who pass login authentication and log in to the NAS. When login authentication is not configured or the authentication exemption method is adopted, EXEC accounting is not performed.
- If accounting start is not performed on a user upon login, accounting stop will not be performed when the user logs out.
- The remote server group method used in the command accounting function supports only the TACACS+ protocol.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an AAA accounting method. Configure at least one of the tasks.

- Configure an EXEC accounting method list.

  aaa accounting exec { **default** | *list-name* } **start-stop** *method*&<1-4>

  NO EXEC accounting method list is configured by default.

  A configured EXEC accounting method list must be applied to a line so that it takes effect.

- Configure a command accounting method list.

  aaa accounting commands *level* { **default** | *list-name* } **start-stop** *method*&<1-4>

  No command accounting method list is configured by default.

  A configured command accounting method list must be applied to a line so that it takes effect.

- Configure a network accounting method list.

  aaa accounting network { **default** | *list-name* } **start-stop** *method*&<1-4>

  No network accounting method list is configured by default.

(4) (Optional) Enable the accounting update function.

aaa accounting update

Accounting update is disabled by default.

After this function is configured, the device updates accounting information periodically. This function helps improve the accounting accuracy. You are advised to configure it.

(5) (Optional) Configure the accounting update interval.

aaa accounting update periodic *interval*

The default accounting update interval is **5** minutes.

It is recommended that the accounting update interval not be configured unless otherwise specified.

(6) Apply the accounting method. Please configure only one task.

- Enter the line configuration mode and apply the EXEC accounting method. Run the following commands in sequence:

  line { **console** | **vty** } *first-line* [*last−line*]

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

  A line is associated with the default method list by default.

- Enter the line configuration mode and apply the command accounting method. Run the following commands in sequence:

  line { **console** | **vty** } *first-line* [*last−line*]

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

  A line is associated with the default method list by default.

- Apply the network accounting method to IEEE 802.1X accounting.

  dot1x accounting { **default** | *list-name* }

  IEEE 802.1X accounting is associated with the default method by default.

1.12 Configuring a Policy for User Accounting Start Failures

1.12.1 Overview

After this function is configured, the user status is online or offline if the accounting start fails.

1.12.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the user online/offline status after the accounting start fails.

aaa accounting start-fail { **offline** | **online** }

The user online/offline status after an accounting start failure is not configured by default.

1.13 Configuring Domain-Based AAA Services

1.13.1 Overview

The domain-based AAA services classify users into different domains and the domains use different security methods to provide AAA services.

1.13.2 Restrictions and Guidelines

- The device supports a maximum of 32 domains.
- After the domain-based AAA services are enabled, if information of a user does not carry domain information, the user is assigned to the default domain **default**. A method list for the **default** domain must be configured on the device. Otherwise, users without domain information cannot use AAA services.

1.13.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable domain-based AAA services.

aaa domain enable

The domain-based AAA services are disabled by default.

(4) Create a domain and enter the domain configuration mode.

aaa domain { **default** | *domain-name* }

No domain is configured by default.

(5) Configure an authentication method list for the AAA domain.

authentication { **dot1x** | **enable** | **login** } { **default** | *list-name* }

The default authentication method list used in an AAA domain is the default method list.

(6) Configure an accounting method list for the AAA domain.

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

The default accounting method list used in an AAA domain is the default method list.

(7) Configure an authorization method list for the AAA domain.

authorization { **commands** | **exec** | **network** } { **default** | *list-name* }

The default authorization method list used in an AAA domain is the default method list.

(8) (Optional) Set the domain status.

state { **active** | **block** }

A configured domain is active by default.

(9) (Optional) Configure whether usernames carry domain name information.

username-format { **with-domain** | **without-domain** }

Usernames carry domain name information during interaction between the NAS and the server by default.

(10) (Optional) Configure a limit on the number of users supported in the domain.

access-limit *access-limit-number*

No limit on the number of users supported in a domain is configured by default.

1.14 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Notice

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

Table 1-1 AAA Monitoring

Command	Purpose
show aaa accounting update	Displays accounting update information.
show aaa domain [**default** | *domain-name*]	Displays information about a configured domain.
show aaa lockout	Displays lockout parameter configuration in the current login authentication.
show aaa group	Displays all AAA server groups.
show aaa method-list	Displays all AAA method lists.
show aaa user { **all** | **by-id** *session-id* | **by-name** *user-name* | **lockout** }	Displays AAA user information.
clear aaa local user lockout { **all** | **user-name** *user-name-id* }	Clears the list of locked users.

1.15 Configuration Examples

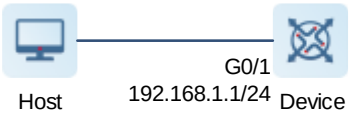
1.15.1 Configuring Local Login Authentication and Local EXEC Authorization

1. Requirements

You can use local login authentication and local EXEC authorization together to control the permissions of users who log in to the device. In this method, you need to configure accounts and their permissions only in the local user database of the device, to control user permissions with no need to use an authentication server.

2. Topology

Figure 1-2 **Topology of Local Login Authentication and Local EXEC Authorization**



3. Notes

- Enable AAA security services on the device.
- Add accounts to the local user database of the device.
- Create an authentication method list and an authorization method list.
- Apply the authentication method and authorization method to a specific line.

4. Procedure

Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

Add accounts **host1** and **host2** to the local user database of the device and configure account permissions.

```
Device(config)# username host1 privilege 15 password password1
Device(config)# username host2 privilege 4 password password2
```

Create a login authentication method list named **login-method**, in which the authentication method is local authentication, and create an EXEC authorization method list named **exec-method**, in which the authorization method is local authorization.

```
Device(config)# aaa authentication login login-method local
Device(config)# aaa authorization exec exec-method local
```

Apply the authentication method list and authorization method list to a line.

```
Device(config)# line vty 0 35
Device(config-line)# login authentication login-method
Device(config-line)# authorization exec exec-method
```

5. Verification

Run the **show aaa method-list** command on the device to display configured method lists.

```
Device# show aaa method-list

Authentication method-list:
aaa authentication login login-method local

Accounting method-list:

Authorization method-list:
aaa authorization exec exec-method local
```

Log in to the device through telnet by using client software (such as PuTTY or Xshell) and verify that different users have different account permissions.

- Log in to the device as user **host1** and check that the privilege level of the user is 15.

```
User Access Verification

Username:host1
Password:password1



Device# show privilege
Current privilege level is 15
```

- Log in to the device as user **host2** and check that the privilege level of the user is 4.

```
User Access Verification

Username:host2
Password:password2



Device# show privilege
Current privilege level is 4
```

6. Configuration Files

```
!
username host1 privilege 15 password password1
username host2 privilege 4 password password2
!
aaa new-model
!
aaa authorization exec exec-method local
aaa authentication login login-method local
!
line vty 0 35
 authorization exec exec-method
 login authentication login-method
!
end
```

7. Common Errors

- No authentication method list and authorization method list are applied to a specific line.
- No account is configured in the local user database.

1.15.2 Configuring Enable Authentication

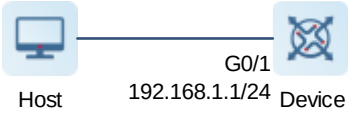
1. Requirements

Users can have execution permissions with a privilege level of 0 to 15. After Enable authentication is configured, users must be authenticated when running the **enable** command to switch the permission to a higher level. As

shown in Figure 1-3, when both local authentication and Enable password authentication are configured on the device, local authentication is preferred. If local authentication is invalid, enable password authentication is used.

2. Topology

Figure 1-3 **Topology of Enable Authentication**



3. Notes

- Enable AAA security services on the device.
- Configure the local user database and Enable password.
- Configure an Enable authentication method list.

Instruction

Only one Enable authentication method list can be defined. Therefore, you do not need to define the name of the Enable authentication method list. After the default method list is configured, the Enable authentication function takes effect automatically.

4. Procedure

Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

Add account **host1** to the local user database and set the privilege level of the account to **15**.

```
Device(config)# username host1 privilege 15 password password1
```

Set the password to **enpassword1** for privilege level 15 in Enable authentication.

```
Device(config)# enable secret level 15 enpassword1
```

Configure an Enable authentication method list, in which local authentication is prior to Enable password authentication.

```
Device(config)# aaa authentication enable default local enable
```

5. Verification

Log in to the device as user **host1** and check that the privilege level of the user is 15.

```
User Access Verification

Username:host1
Password:password1
```

```
Device# show privilege
Current privilege level is 15
```

Switch the privilege level to 4 and verify that no password is required for authentication.

```
Device# enable 4
Device# show privilege
Current privilege level is 4
```

Switch the privilege level to 15 and verify that identity authentication is needed. Local authentication has a higher priority. Therefore, you can enter the password of **host1** (**password1**) for authentication to successfully switch the privilege level to 15.

```
Device# enable 15
Password:password1

Device# show privilege
Current privilege level is 15
```

6. Configuration Files

```
!
username host1 privilege 15 password password1
!
aaa new-model
!
aaa authentication enable default local enable
!
enable secret 5 $1$7b8Y$v6u11F23p9y3vwp6
!
end
```

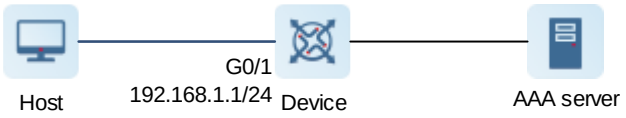
1.15.3 Configuring Network Authorization

1. Requirements

Network authorization needs to be configured to grant available network services to users, such as the traffic, bandwidth, and timeout services.

2. Topology

Figure 1-4 **Topology of Network Authorization**



3. Notes

- Enable AAA security services.
- Configure a network authorization method list.

- Apply the network authorization method list to a specific interface line (skip this step if you configure the default method).

4. Procedure

Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

Configure the default network authorization method list.

```
Device(config)# aaa authorization network default group radius none
```

5. Verification

Run the **show aaa method-list** command on the device to display configuration results.

```
Device# show aaa method-list

Authentication method-list:

Accounting method-list:

Authorization method-list:
aaa authorization network default group radius none
```

6. Configuration Files

```
!
aaa new-model
!
aaa authorization network default group radius none
!
```

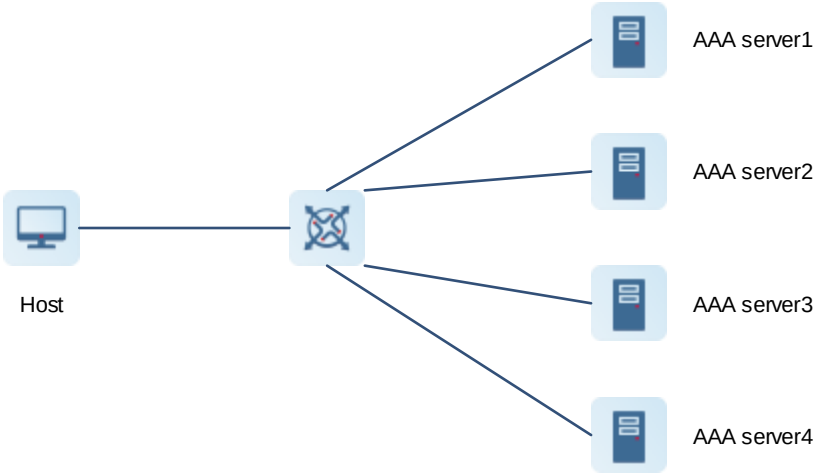
1.15.4 Configuring an AAA Server Group

1. Requirements

A custom AAA server group needs to be created to provide AAA services.

2. Topology

Figure 1-5 **Topology of an AAA Server Group**



3. Notes

- Configure AAA servers.
- Create an AAA custom server group.
- Add server group members to the custom server group.

4. Procedure

(1) Add AAA servers (the following uses RADIUS servers as an example).

```
Device> enable
Device# configure terminal
Device(config)# radius-server host 10.1.1.1
Device(config)# radius-server host 10.1.1.2
Device(config)# radius-server host 10.1.1.3
Device(config)# radius-server host 10.1.1.4
```

(2) Configure a global RADIUS server communication key.

```
Device(config)# radius-server key radiuskey
```

(3) Create a server group named **group1** and add members to the group.

```
Device(config)# aaa group server radius group1
Device(config-gs-radius)# server 10.1.1.1
Device(config-gs-radius)# server 10.1.1.2
Device(config-gs-radius)#exit
```

(4) Create a server group named **group2** and add members to the group.

```
Device(config)#aaa group server radius group2
Device(config-gs-radius)#server 10.1.1.3
Device(config-gs-radius)#server 10.1.1.4
Device (config-gs-radius)#exit
```

5. Verification

Run the **show aaa group** command on the device to display the configuration results.

```
Device# show aaa group
Type       Reference  Name
---------- ---------- ----------
radius     1          radius
tacacs+    1          tacacs+
radius     1          group1
radius     1          group2
```

6. Configuration Files

```
!
radius-server host 10.1.1.1
radius-server host 10.1.1.2
radius-server host 10.1.1.3
radius-server host 10.1.1.4
radius-server key radiuskey
!
aaa group server radius group1
 server 10.1.1.1
 server 10.1.1.2
!
aaa group server radius group2
 server 10.1.1.3
 server 10.1.1.4
!
```

7. Common Errors

For RADIUS servers that use non-default authentication ports and non-default accounting ports, the authentication port or accounting port is not specified when the **server** command is run to add servers.

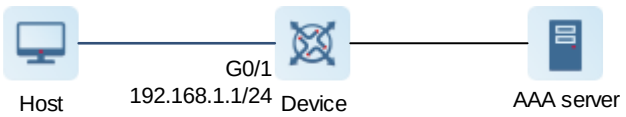
1.15.5 Configuring Domain-based AAA Services

1. Requirements

After a domain is created and a security method list is specified for the domain, users belonging to the domain use security methods of the domain for authentication, authorization, and accounting.

2. Topology

Figure 1-6 **Topology of Domain-Based AAA Services**



3. Notes

- Configure a RADIUS server in advance so that RADIUS server authentication and accounting can be performed.
- Enable AAA security services.
- Configure an AAA security method list.
- Enable domain-based AAA services.
- Create a domain.
- Associate the AAA security method list with the domain.
- Configure domain attributes.

4. Procedure

(1) Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

(2) Configure an AAA server (the following uses the RADIUS server as an example).

```
Device(config)# radius-server host 192.168.1.2 key radiuskey
```

(3) Configure an AAA security method list.

```
Device(config)# aaa authentication dot1x default group radius
Device(config)# aaa accounting network list3 start-stop group radius
```

(4) Enable domain-based AAA services.

```
Hostname(config)# aaa domain enable
```

(5) Create a domain and configure domain attributes.

```
Device(config)# aaa domain domain.com
Device(config-aaa-domain)# authentication dot1x default
Device(config-aaa-domain)# accounting network list3
Device(config-aaa-domain)# username-format without-domain
```

5. Verification

Run the **show aaa domain** command on the device to display domain configuration.

```
Device# show aaa domain domain.com

=============Domain domain.com=============
State: Active
Username format: With-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
 accounting network list3
```

6. Configuration Files

```
!
aaa new-model
aaa domain enable
!
aaa domain domain.com
 authentication dot1x default
 accounting network list3
 username-format without-domain
!
aaa accounting network list3 start-stop group radius
aaa authentication dot1x default group radius
!
radius-server host 192.168.1.2 key radiuskey
!
```

1.16 Common Errors

- When a local method is configured to provide AAA security services, no user information is configured in the local database.
- When a remote server group method is configured to provide AAA security services, no RADIUS/TACACS+ server is configured and no user information is configured on the server.

Contents

1 Configuring RADIUS 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 8
1.2 Configuration Task Summary 8
1.3 Configuring RADIUS Basic Features 8
1.3.1 Overview 8
1.3.2 Restrictions and Guidelines 8
1.3.3 Procedure 9
1.4 Configuring a RADIUS Server Group 10
1.4.1 Overview 10
1.4.2 Restrictions and Guidelines 10
1.4.3 Procedure 10
1.5 Configuring RADIUS Attributes 11
1.5.1 Overview 11
1.5.2 Configuration Tasks 11
1.5.3 Configure the Attribute Format 11
1.5.4 Configuring Ruijie Private Attributes 12
1.5.5 Configuring Compatibility with Devices of Other Vendors 12
1.6 Configuring RADIUS Reachability Detection 13
1.6.1 Overview 13
1.6.2 Restrictions and Guidelines 13

1.6.3 Procedure....14

1.7 Configuring the DSCP Value for RADIUS Packets....15

1.7.1 Overview....15

1.7.2 Procedure....15

1.8 Configuring the Units of Data Flows and Packets to Be Sent to a RADIUS Server....15

1.8.1 Overview....15

1.8.2 Procedure....15

1.9 Configuring the Accounting-On Function....15

1.9.1 Overview....15

1.9.2 Procedure....16

1.10 Configuring the Accounting Packet Copying Function....16

1.10.1 Overview....16

1.10.2 Procedure....16

1.11 Monitoring....16

1.12 Configuration Examples....17

1.12.1 Configuring RADIUS Authentication, Authorization, and Accounting....17

1.12.2 Configuring RADIUS Reachability Detection....19

1 Configuring RADIUS

1.1 Introduction

1.1.1 Overview

The Remote Authentication Dial-In User Service (RADIUS) is a distributed authentication, authorization and accounting (AAA) protocol based on the client/server architecture. It works with AAA to provide AAA security services for users.

When providing AAA security services, a network device serves as a RADIUS client to provide user information to the RADIUS server to initiate security service requests. The remote RADIUS server stores user information and network service information, and provides security services for users by responding to requests from the RADIUS client.

RADIUS is usually applied in networks that have high security requirements and allow remote user access. As a completely open protocol, many systems (such as UNIX, Windows 2000, and Windows 2008) support the installation of RADIUS as a system component. Therefore, the RADIUS server becomes the most widely used security server.

1.1.2 Principles

1. Basic Concepts

- Client/server mode

  RADIUS uses the client/server mode and consists of RADIUS clients and the RADIUS server.

  - As the initiator of RADIUS requests, a RADIUS client usually runs on a network access server (NAS). It provides user information for the RADIUS server, and receives and processes responses from the RADIUS server, for example, accepting or rejecting user access, and requesting user-specific information.
  - The RADIUS server maintains the IP addresses and shared key of RADIUS clients as well as configured user information, and provides authentication, authorization, and accounting services by responding to requests from RADIUS clients. One RADIUS server usually corresponds to multiple RADIUS clients.

- Shared key

  A shared key is a string shared between a RADIUS client and the server. It is used to encrypt and decrypt user passwords during RADIUS packet transmission and generate packet verification fields, in an effort to ensure RADIUS communication security.

- RADIUS server group

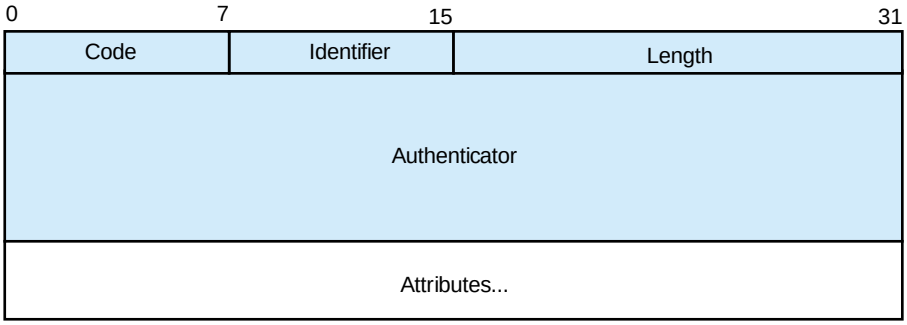
  Security methods used in AAA security services are based on server groups. Likewise, RADIUS provides AAA security services based on RADIUS server groups. One security method corresponds to one RADIUS server group and one or more RADIUS severs can be configured in each RADIUS server group.

  If multiple RADIUS servers are configured in a RADIUS server group, when a device fails to communicate with the first RADIUS server or the first RADIUS server is unreachable, the device automatically attempts to communicate with the second RADIUS server, and so on. The attempt lasts till the communication succeeds or the communication with all RADIUS servers fails.

2. RADIUS Packet

- Packet structure

Figure 1-1 Structure of a RADIUS Packet



Fields contained in the packet structure shown in Figure 1-1 are described in Table 1-1.

Table 1-1 Description of Fields Contained in a RADIUS Packet

Field	Length	Description	Remarks
Code	1 byte	Identifies the packet type.	Values corresponding to common packet types and their meanings are as follows: **1**: Access-Request **2**: Access-Accept **3**: Access-Reject **4**: Accounting-Request **5**: Accounting-Response **11**: Access-Challenge
Identifier	1 byte	Matches a request with a response packet.	Request packets and response packets of the same type have the same identifier value.
Length	2 bytes	Indicates the length of a RADIUS packet.	The value is the sum of the lengths of the **Code**, **Identifier**, **Length**, **Authenticator**, and **Attributes** fields. If the length of a received packet is greater than the value of **Length**, the content beyond the value of **Length** is ignored as filling information. If the length of a received packet is smaller than the value of **Length**, the packet is discarded.

Field	Length	Description	Remarks
Authenticator	16 bytes	Verifies packets and encrypts and decrypts user passwords.	N/A
Attributes	Variable length	Carries authentication, authorization, and accounting information.	This field usually contains multiple attributes and each attribute is represented in the type, length, value (TLV) format.

- RADIUS attributes

  RADIUS attributes carry authentication, authorization, and accounting information, and each attribute is represented in the TLV format, as described in Table 1-2.

Table 1-2 Description of RADIUS Attribute Fields

Field	Length	Description
Type	1 byte	Attribute type
Length	1 byte	Total length of an attribute (TLV)
Value	Variable length	Attribute description

Table 1-3 RADIUS Attribute List

Attribute No.	Attribute Name	Attribute No.	Attribute Name
1	User-Name	43	Acct-Output-Octets
2	User-Password	44	Acct-Session-Id
3	CHAP-Password	45	Acct-Authentic
4	NAS-IP-Address	46	Acct-Session-Time
5	NAS-Port	47	Acct-Input-Packets
6	Service-Type	48	Acct-Output-Packets
7	Framed-Protocol	49	Acct-Terminate-Cause
8	Framed-IP-Address	50	Acct-Multi-Session-Id
9	Framed-IP-Netmask	51	Acct-Link-Count
10	Framed-Routing	52	Acct-Input-Gigawords
11	Filter-ID	53	Acct-Output-Gigawords
12	Framed-MTU	55	Event-Timestamp
13	Framed-Compression	60	CHAP-Challenge

Attribute No.	Attribute Name	Attribute No.	Attribute Name
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
18	Reply-Message	64	Tunnel-Type
19	Callback-Number	65	Tunnel-Medium-Type
20	Callback-ID	66	Tunnel-Client-Endpoint
22	Framed-Route	67	Tunnel-Server-Endpoint
23	Framed-IPX-Network	68	Acct-Tunnel-Connection
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access
28	Idle-Timeout	73	ARAP-Security
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference
39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Response
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Lost
42	Acct-Input-Octets	87	NAS-Port-Id

- Introduction to RADIUS attributes

  This section describes some of the important attributes.

  - Attribute 31

  When a RADIUS client sends a request packet to the RADIUS server, information is filled in attribute 31 (**Calling-Station-ID**) to identify the user to be authenticated. The MAC address of a user is often used as the attribute content. For example, in IEEE 802.1X authentication, the device uses the MAC address of the device where the IEEE 802.1X client resides as the attribute content.

Different RADIUS servers have different requirements for the format of the MAC address in attribute 31. Therefore, ensure that the MAC address format used by RADIUS clients is the same as that used by the server. Currently, the following three MAC address formats are supported.

Table 1-4 Supported Formats of the MAC Address in Attribute 31

MAC Address Format	Description
ietf	Standard format specified in the Internet Engineering Task Force (IETF) standard (RFC3580). It uses hyphens (-) as the separator, for example, 00-D0-F8-33-22-AC.
normal	Dotted hexadecimal format using dots (.) as the separator, for example, 00d0.f833.22ac.
unformatted	Default format with no separator, for example, 00d0f83322ac.

- Attribute 26

Attribute 26 (**Vendor-Specific**) is also called a private attribute, which allows device vendors to define attributes. Device vendors can define multiple attributes in the TLV format in attribute 26. Table 1-5 lists private attributes supported by Ruijie products.

Table 1-5 List of Ruijie Private Attributes

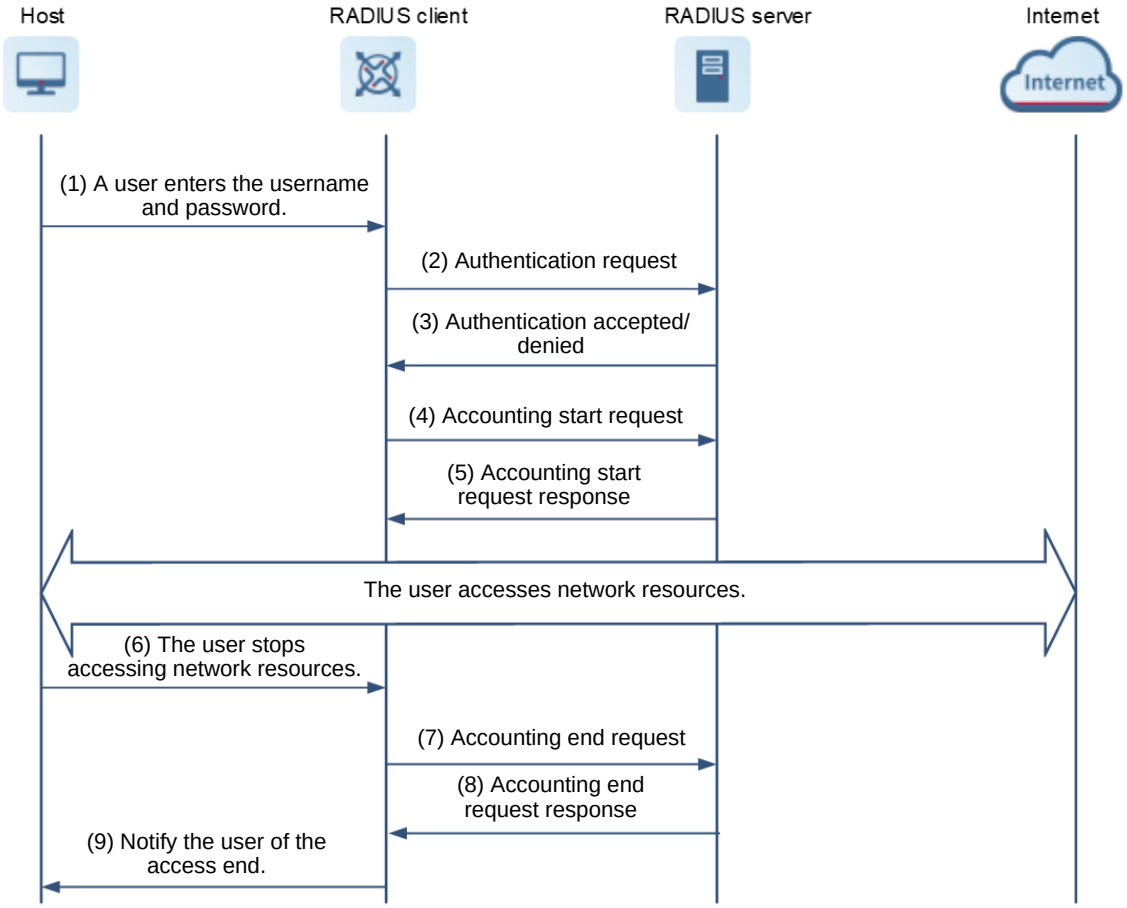
ID	Function	Type	Extended Type
1	max-down-rate	1	76
2	port-priority	2	77
3	user-ip	3	3
4	VLAN-id	4	4
5	last-supplicant-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	file-name-4	15	15
16	max-up-rate	16	16
17	current-supplicant-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20

ID	Function	Type	Extended Type
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42
26	IPv6-multicast-address	79	79
27	IPv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

3. RADIUS Authentication, Authorization, and Accounting

RADIUS provides authentication, authorization, and accounting for users. The interaction process is shown in Figure 1-2.

Figure 1-2 RADIUS Authentication, Authorization, and Accounting Process



- RADIUS authentication and authorization process

  a A user enters the username and password and sends them to a RADIUS client.

b After receiving the username and password, the RADIUS client sends an authentication request packet to the RADIUS server. The password in the authentication request packet is encrypted.

c After receiving the authentication request, the RADIUS server checks whether the username and password are legitimate. If yes, the RADIUS server accepts the authentication request and delivers authorization information of the user. If no, the RADIUS server rejects the authentication request.

- RADIUS accounting process

  a If the RADIUS server returns an authentication success message in the user authentication process, the RADIUS client sends an accounting start request packet to the RADIUS server.

  b The RADIUS server returns an accounting start response packet and starts accounting.

  c When stopping accessing network resources, the user sends a disconnection request to the RADIUS client.

  d The RADIUS client sends an accounting end request packet to the RADIUS server.

  e The RADIUS server returns an accounting end response packet and stops accounting.

  f The user is disconnected from the network and cannot access network resources.

4. RADIUS Packet Retransmission Upon Timeout

After sending a packet to the RADIUS server, a RADIUS client uses a timer to test whether the RADIUS server responds within the specified time. If the RADIUS server does not respond within the specified time, the RADIUS client retransmits the packet. The following timeout and retransmission parameters need to be configured:

- RADIUS server timeout duration

  The response time of a RADIUS server depends on its performance and the network environment. Configure a proper timeout duration based on the actual situation.

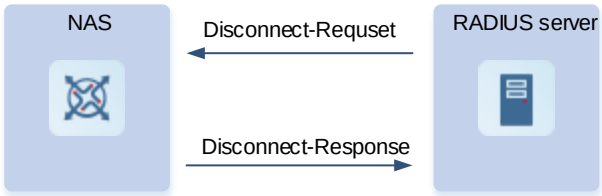
- Retransmission count
- Whether accounting update packets need to be retransmitted

5. RADIUS Forcible Logoff

Users can go offline actively. In addition, the RADIUS server can send messages to force authenticated users offline.

RADIUS forcible logoff is a user logoff management method defined in the protocol of Dynamic Authorization Extensions to RADIUS. The NAS and RADIUS server exchange Disconnect-Messages (DMs) to force authenticated users offline. The protocol of Dynamic Authorization Extensions to RADIUS enables NASs from different vendors to be compatible with RADIUS servers in user logoff processing.

Figure 1-3 DM Interaction of Dynamic Authorization Extensions to RADIUS



The DM interaction between a RADIUS server and the NAS is as follows:

(1) The RADIUS server actively sends a Disconnect-Request message to port UDP3799 of the NAS to initiate a user logoff request.

(2) The NAS searches for the user based on the user session information and username carried in the Disconnect-Request message and logs off the user.

(3) The NAS sends the logoff result to the RADIUS server through a Disconnect-Response message.

1.1.3 Protocols and Standards

- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868: RADIUS Attributes for Tunnel Protocol Support
- RFC2869: RADIUS Extensions
- RFC3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

1.2 Configuration Task Summary

RADIUS configuration includes the following tasks:

(1) Configuring RADIUS Basic Features

(2) Configuring a RADIUS Server Group

(3) (Optional) Configuring RADIUS Attributes Select at least one of the following tasks to configure.

- Configure the Attribute Format
- Configuring Ruijie Private Attributes
- Configuring Compatibility with Devices of Other Vendors

(4) (Optional) Configuring RADIUS Reachability Detection

(5) (Optional) Configuring the DSCP Value for RADIUS Packets

(6) (Optional) Configuring the Units of Data Flows and Packets to Be Sent to a RADIUS Server

(7) (Optional) Configuring the Accounting-On Function

(8) (Optional) Configuring the Accounting Packet Copying Function

1.3 Configuring RADIUS Basic Features

1.3.1 Overview

This section describes how to configure parameters for the communication between a network device and a RADIUS server to ensure normal communication between them. After the parameters are configured, the device can correctly send AAA authentication, authorization, and accounting requests to the RADIUS server and give responses.

1.3.2 Restrictions and Guidelines

- Before configuring RADIUS, ensure that the network communication between the device and the RADIUS server is in good condition.

- Before configuring RADIUS IPv6 authentication, ensure that the RADIUS server supports RADIUS IPv6 authentication.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a RADIUS remote server.

radius-server host [**oob** [**via Mgmt** *Mgmt_number*]] { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port-number* | **acct-port** *acct-port-number*] * [**test username** *username* [**ignore-acct-port**] [**ignore-auth-port**] [**idle-time** *idle-time*]] [**key** [**0** | **7**] *text-string*]

No RADIUS remote server is configured by default.

If a RADIUS server is not added to a RADIUS server group, the device uses the global routing table when communicating with the RADIUS server. Otherwise, the device uses the virtual routing and forwarding (VRF) routing table of the RADIUS server group.

(4) Configure a shared key for the communication between the device and the RADIUS server.

radius-server key [**0** | **7**] *key*

No shared key for the communication between the device and the RADIUS server is configured by default.

A shared key is the basis for correct communication between the device and the RADIUS server. The same shared key must be configured on them both to ensure normal communication between them.

(5) (Optional) Configure the source address for RADIUS packets.

ip radius source-interface *interface-type interface-number*

The source IP address of RADIUS packets is set by the network layer by default.

After this command is configured, the device uses the first IP address of the interface specified in the command as the source address of RADIUS packets. Ensure that the communication between the configured address and the RADIUS server is normal. Specifying the source IP address for packets to be sent to the RADIUS server can reduce the NAS information maintenance workload on the RADIUS server.

(6) (Optional) Configure the source UDP port to be used by the device to send RADIUS packets.

radius-server source-port *source-port*

The source UDP port used by the device to send RADIUS packets is a random packet by default.

(7) (Optional) Configure the waiting time, after which the device retransmits a RADIUS request packet.

radius-server timeout *timeout*

The default waiting time before the retransmission of a RADIUS packet is **5** seconds.

(8) (Optional) Configure the accounting update packet retransmission function for Web-authenticated users.

radius-server account update retransmit

The accounting update packet retransmission function is enabled for Web-authenticated users by default.

The configuration does not affect users of other authentication types.

1.4 Configuring a RADIUS Server Group

1.4.1 Overview

One or more RADIUS servers can be added to each RADIUS server group, which provides AAA services for users as a whole.

1.4.2 Restrictions and Guidelines

- RADIUS security services are a type of AAA services and need to be used in combination with AAA features. RADIUS provides security services for users as one method in an AAA method list.
- When configuring the authentication and accounting method lists, you can specify server groups separately for them.
- In a user-defined server group, you can only specify and apply servers in the default server group.
- RADIUS server groups support VRF instances. When a server group in a specified VRF instance is used, the source address used by the device to communicate with a remote server must be obtained from the VRF instance. If you run the **ip radius source-interface** command to specify the source interface for request packets, the IP address obtained from this source interface takes priority over that found in the VRF instance.
- The name of a server group cannot be set to the predefined keyword **radius**.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a RADIUS server group.

aaa group server radius *group-name*

No RADIUS server group is configured by default.

You can group RADIUS servers so that authentication and accounting can be completed by different server groups.

(4) Add a server to the RADIUS server group.

server { *ipv4-address* | *ipv6-address* }

No server is added to a RADIUS server group by default.

(5) (Optional) Specify a VRF instance for the RADIUS server group.

ip vrf forwarding *vrf-name*

No VRF instance is specified for a RADIUS server group by default.

The VRF instance specified for a RADIUS server group must use a valid name configured using the **vrf definition** command in global configuration mode.

(6) (Optional) Configure an MGMT port to be used by the RADIUS server group.

ip oob [**via Mgmt** *mgmt-number*]

No MGMT port to be used by a RADIUS server group is configured by default.

1.5 Configuring RADIUS Attributes

1.5.1 Overview

RADIUS attributes are used to carry authentication, authorization, and accounting information to be used in packet interaction. You can configure the attribute format, private attribute processing method, and vendor compatibility.

1.5.2 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configure the Attribute Format
- Configuring Ruijie Private Attributes
- Configuring Compatibility with Devices of Other Vendors

1.5.3 Configure the Attribute Format

1. Overview

This section describes how to configure the attribute format to be used in encapsulation and parsing.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure RADIUS attributes. Configure at least one of the tasks.

- Configure the format of the MAC address used in attribute 31 (**Calling-Station-ID**).

  radius-server attribute 31 mac format { **3hyphen** | **ietf** | **normal** | **unformatted** | { { **colon-split** | **dot-split** | **hyphen-split** } { **mode1** | **mode2** } [**lowercase** | **uppercase**] } }

  The MAC address used in attribute 31 uses the unformatted pattern.

  Some RADIUS servers (mainly used for IEEE 802.1X authentication) can identify only MAC addresses in the IETF format. In this case, set the format of MAC addresses used in attribute 31 to the IETF format.

- Configure the encapsulation format for the **NAS-Port-ID** attribute.

  radius-server attribute nas-port-id format { **mode**1 | **normal** | **port-vid** | **qinq** }

  The default encapsulation format of the **NAS-Port-ID** attribute is the normal format.

  Use this command to configure the encapsulation format for the **NAS-Port-ID** attribute applicable to 802.1Q in 802.1Q (QinQ) scenarios or non-QinQ scenarios.

- Configure the parsing mode for the **Class** attribute.

  radius-server attribute class user-flow-control { **format-16bytes** | **format-32bytes** | **unit bit/s** | **unit byte/s** }

  The function of parsing the rate limit configuration from the **Class** attribute of RADIUS packets is disabled by default.

  Configure this command if a server needs to deliver the rate limit value by using the **Class** attribute.

- Configure whether RADIUS authentication request packets carry a specified attribute.

radius-server authentication attribute *type* { **package** | **unpackage** }

According to the RFC standard, attributes that must be carried in authentication requests are carried by default, attributes that do not need to be carried are not carried by default, and other attributes are in the unset state by default.

- Configure whether RADIUS accounting request packets carry a specified attribute.

  radius-server account attribute *type* { **package | unpackage** }

  According to the RFC standard, attributes that must be carried in accounting requests are carried by default, attributes that do not need to be carried are not carried by default, and other attributes are in the unset state by default.

1.5.4 Configuring Ruijie Private Attributes

1. Overview

Vendors can define private attributes to implement some features that are not supported by the standard RADIUS protocol. You can configure the methods used by devices to process private attributes based on the actual environment. Private attributes configured in this section are all Ruijie private attributes.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure Ruijie private attributes. Configure at least one of the tasks.

- Configure the device to set the private attribute **port-priority** delivered by the server to the class of service (CoS) value of an interface.

  radius set qos cos

  The device sets the private attribute **port-priority** delivered by the server to the differentiated services code point (DSCP) value by default.

- Configure the device to support the **CUI** attribute.

  radius support cui

  The function of supporting the **CUI** attribute by RADIUS is disabled by default.

1.5.5 Configuring Compatibility with Devices of Other Vendors

1. Overview

In actual deployment environments, Ruijie devices may interconnect to RADIUS servers of other vendors. Private attributes defined by different vendors are different. It is necessary to enable compatibility with the configuration of devices of other vendors.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure compatibility with devices of other vendors. Configure at least one of the tasks.

- Configure whether RADIUS authentication request packets carry the private attributes of a specified vendor.

  radius-server authentication vendor { **cisco | cmcc** | **microsoft** } **package**

  Authentication request packets do not carry private attributes of other vendors by default.

- Configure whether RADIUS accounting request packets carry the private attributes of a specified vendor.

  radius-server account vendor { **cisco | cmcc** | **microsoft** } **package**

  Accounting request packets do not carry private attributes of other vendors by default.

- Configure RADIUS to parse private attributes of Cisco, Huawei, and Microsoft devices carried in packets.

  radius vendor-specific attribute support { **cisco** | **huawei** | **ms** }

  RADIUS parses private attributes of Cisco, Huawei, and Microsoft devices carried in packets by default.

- Enable the function of not differentiating private vendor IDs during RADIUS packet parsing.

  radius vendor-specific extend

  RADIUS identifies only Ruijie private vendor ID during packet parsing by default.

- Configure the mode of parsing private attributes.

  radius vendor-specific attribute support { **cisco** | **huawei** | **ms** }

  RADIUS parses private attributes of Cisco, Huawei, and Microsoft devices carried in packets by default.

  If the server is a Ruijie application server, the RADIUS private attribute type needs to be configured to achieve compatibility.

1.6 Configuring RADIUS Reachability Detection

1.6.1 Overview

A RADIUS server can be only in the reachable or unreachable state. The device will not send authentication, authorization, or accounting requests of access users to an unreachable RADIUS server unless all servers in the RADIUS server group are unreachable.

The device maintains the reachability status of each RADIUS server. The device selects a reachable RADIUS server preferentially to improve the handling performance of RADIUS services.

The device actively detects whether a specified RADIUS server is reachable. After the active detection function is configured, the device periodically sends detection requests (authentication requests or accounting requests) to the RADIUS server. The active detection interval is **60** minutes when the RADIUS server is reachable and **1** minute when the RADIUS server is unreachable.

1.6.2 Restrictions and Guidelines

- To enable active detection for a specified RADIUS server, perform the following configuration when configuring the RADIUS server:
  - Configure a test username for the RADIUS server.
  - Configure at least one tested port (authentication port or accounting port) for the RADIUS server.

- It is judged that a RADIUS server is unreachable only when both conditions below are met:
  - The device fails to receive a correct response packet from the RADIUS server within the specified timeout duration.
  - The number of times that the device sends request packets to the same RADIUS server consecutively reaches the specified timeout count.
- If any of the following conditions is met for an unreachable RADIUS server, the RADIUS server is considered reachable.
  - The device receives correct responses from the RADIUS server.
  - The duration in which the RADIUS server is unreachable exceeds the time configured using the **radius-server deadtime** command, and active detection is disabled for the RADIUS server.
  - The authentication port or accounting port of the RADIUS server is updated on the device.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the criteria for the device to judge that a RADIUS server is unreachable.

radius-server dead-criteria { **time** *timeout* | **tries** *tries-number* | **time** *timeout* **tries** *tries-number* }

The criteria for judging that a RADIUS server is unreachable are that the timeout duration is 60 seconds and the consecutive timeout count is 10 by default.

If a RADIUS server meets both the duration condition and the consecutive request timeout count condition, it is deemed that the RADIUS server is unreachable.

(4) Configure active detection and set the IP address, authentication port, or accounting port for the remote RADIUS server.

radius-server host { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port-number* | **acct-port** *acct-port-number*] *

No active detection is configured by default.

(5) (Optional) Configure the number of times that the device sends requests to a RADIUS server consecutively before confirming that the RADIUS server is unreachable.

radius-server retransmit *retransmit-times*

The device sends requests to a RADIUS server three times consecutively before confirming that the RADIUS server is unreachable by default.

(6) (Optional) Configure the duration for the device to stop sending request packets to an unreachable RADIUS server.

radius-server deadtime *deadtime*

Even if a RADIUS server is unreachable, the device still sends requests to the RADIUS server by default.

If active detection is enabled for a RADIUS server, the time parameter configured by the **radius-server deadtime** command does not take effect on the RADIUS server.

1.7 Configuring the DSCP Value for RADIUS Packets

1.7.1 Overview

DSCP is in the type of service (ToS) field of the IP header and is used to identify the packet transmission priority. A larger DSCP value indicates a higher packet priority. The default DSCP value of RADIUS packets is **0**. You can configure the DSCP value for RADIUS packets to change the transmission priority of RADIUS packets.

1.7.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the DSCP value for RADIUS packets.

radius dscp *dscp-value*

The default DSCP value of RADIUS packets is **0**.

1.8 Configuring the Units of Data Flows and Packets to Be Sent to a RADIUS Server

1.8.1 Overview

The default units of data flows and data packets to be sent to a RADIUS server are bytes and packets respectively. You can configure the units of data flows and data packets to be sent to a RADIUS server based on the actual network situation.

1.8.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the units of data flows and data packets to be sent to a RADIUS server.

radius data-flow-format { { **data byte** | **data giga-byte** | **data kilo-byte** | **data mega-byte** } | { **packet giga-packet** | **packet kilo-packet** | **packet mega-packet** | **packet one-packet** } } *

The default units of data flows and data packets to be sent to a RADIUS server are bytes and packets respectively.

1.9 Configuring the Accounting-On Function

1.9.1 Overview

The accounting-on function is used to notify a RADIUS server of the device restart. After the device is restarted, online users are forced offline. However, the RADIUS server does not perceive the device restart and does not

log off the users. As a result, the users encounter an exception when initiating re-authentication. Therefore, it is necessary to enable the accounting-on function.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the function of sending accounting-on packets upon device restart.

radius-server accounting-on enable

The function of sending accounting-on packets upon device restart is enabled by default.

1.10 Configuring the Accounting Packet Copying Function

1.10.1 Overview

RADIUS accounting packets are sent to one server specified in the accounting method list by default. After this function is enabled, the device copies accounting packets and sends the packets to all servers in a server group.

1.10.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the function of copying and sending accounting packets to servers in a specified group.

radius-sever accounting-copy *group*

The function of copying and sending RADIUS accounting packets is disabled by default.

1.11 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Run the **debug** commands to output debugging information.

Notice

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

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-6 RADIUS Monitoring

Command	Purpose
show radius parameter	Displays global parameters of a RADIUS server.
show radius server	Displays the configuration of a RADIUS server.
show radius vendor-specific	Displays the configuration of the RADIUS private attribute type.
show radius auth statistics	Displays RADIUS authentication statistics.
show radius radius acct statistics	Displays RADIUS accounting statistics.
show radius group	Displays the configuration of a RADIUS server group.
show radius attribute	Displays RADIUS standard attributes.
show radius-server accounting-copy	Displays the configuration of copying and sending the accounting packets.
debug radius detail	Debugs RADIUS packets.
debug radius extend event	Debugs the function of Dynamic Authorization Extensions to RADIUS.
debug radius extend detail	Debugs packets of Dynamic Authorization Extensions to RADIUS.
debug radius extend error	Prints information related to packets of Dynamic Authorization Extensions to RADIUS for debugging.

1.12 Configuration Examples

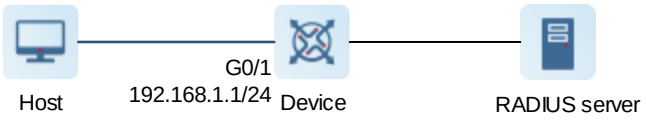
1.12.1 Configuring RADIUS Authentication, Authorization, and Accounting

1. Requirements

A RADIUS server needs to be used for authentication, authorization, and accounting of login users.

2. Topology

Figure 1-4 Topology of RADIUS Authentication, Authorization, and Accounting



3. Notes

- Configure device information and add login users on the RADIUS server.
- Enable AAA security services on the device.

- Configure RADIUS server information on the device.
- Configure the RADIUS authentication method list, authorization method list, and accounting method list.
- Apply the RADIUS authentication, authorization, and accounting methods to a specific line.

4. Procedure

(1) Configure device information and add login users on the RADIUS server. The configuration is omitted here. For details, see the RADIUS server configuration manual.

(2) Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

(3) Configure a RADIUS server (the IP address of the RADIUS server is set to 192.168.1.3 and the shared key is set to **sharekey** here).

```
Device(config)# radius-server host 192.168.1.3 key sharekey
```

(4) Configure the authentication, authorization, and accounting method lists.

```
Device(config)# aaa authentication login radius-method group radius
Device(config)# aaa authorization exec radius-method group radius
Device(config)# aaa accounting exec radius-method start-stop group radius
```

(5) Apply the authentication, authorization, and accounting methods to a line.

```
Device(config)# line vty 0 4
Device(config-line)# login authentication radius-method
Device(config-line)# authorization exec radius-method
Device(config-line)# accounting exec radius-method
```

5. Verification

After entering the correct username and password, a user can log in to the device successfully.

```
User Access Verification

Username:hostname1
Password:password1



Device#
```

After login, the user has only the privilege level granted by the server and can run commands only under this privilege level.

After the user logs out, accounting information of the user can be queried on the RADIUS server. For details about how to query accounting information, see the RADIUS server configuration manual.

6. Configuration Files

```
!
aaa new-model
!
aaa accounting exec radius-method start-stop group radius
```

```
aaa authorization exec radius-method group radius
aaa authentication login radius-method group radius
!
radius-server host 192.168.1.3 key 7 $10$275$g8oXDDIPVeA=$
!
line console 0
line vty 0 4
 accounting exec radius-method
 authorization exec radius-method
 login authentication radius-method
!
```

7. Common Errors

The shared key configured on the device is inconsistent with that used by the RADIUS server.

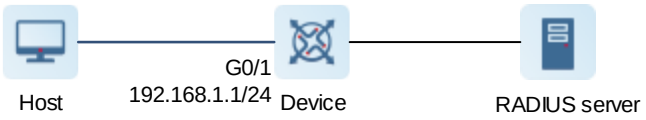
1.12.2 Configuring RADIUS Reachability Detection

1. Requirements

RADIUS reachability detection needs to be configured to identify unreachable RADIUS servers.

2. Topology

Figure 1-5 Topology of RADIUS Reachability Detection



3. Notes

- Configure the global criteria for judging that a RADIUS server is unreachable.
- Configure an IP address for the RADIUS server and configure active detection parameters.

4. Procedure

Configure the global criteria for judging that a RADIUS server is unreachable as follows: The consecutive timeout count is **5** and the timeout duration is **120** seconds.

```
Device> enable
Device# configure terminal
Device(config)# radius-server dead-criteria time 120 tries 5
```

Set the IP address of the RADIUS server to 192.168.1.3, detection username to **test**, and detection interval to **90** minutes, and disable the server authentication port detection.

```
Device(config)# radius-server host 192.168.1.3 test username test ignore-acct-
port idle-time 90
```

5. Verification

Disconnect the network communication between the device and the server with the IP address 192.168.1.3. Initiate RADIUS authentication through the device. After 120 seconds, run the **show radius server** command to check that the server status is "Dead".

```
Hostname# enable
Hostname# show radius server

Server IP:   192.168.1.3
Accounting Port:  1813
Authen  Port:    1812
mom    flag:    1
Test Username:   test
Test Idle Time:   1 Minutes
Test Ports:      Authen and Accounting
Server State:    Dead
   Current duration 1254s, previous duration 2918s
   Dead: total time 1257s, count 1
   Statistics:
      Authen: request 22, timeouts 81
      Author: request 22, timeouts 81
      Account: request 23, timeouts 83
```

6. Configuration Files

```
!
radius-server host 192.168.1.3 test username test ignore-acct-port idle-time 90
key 7 $10$275$g8oXDDIPVeA=$
radius-server dead-criteria time 120 tries 5
!
```

Contents

1 Configuring TACACS.....1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles.....1

1.1.3 Protocols and Standards 4

1.2 Configuration Task Summary 4

1.3 Configuring TACACS+ Basic Features 5

1.3.1 Overview 5

1.3.2 Restrictions and Guidelines 5

1.3.3 Procedure.....5

1.4 Configuring TACACS+ Reachability Detection 6

1.4.1 Overview 6

1.4.2 Restrictions and Guidelines 6

1.4.3 Procedure.....6

1.5 Configuring a TACACS+ Server Group.....7

1.5.1 Overview 7

1.5.2 Restrictions and Guidelines 7

1.5.3 Procedure.....7

1.6 Monitoring 8

1.7 Configuration Examples.....8

1.7.1 Configuring TACACS+ for Login Authentication 8

1.7.2 Configuring Separated Authentication, Authorization and Accounting by Using TACACS+ 10

1.7.3 Configuring Reachability Detection 12

1 Configuring TACACS

1.1 Introduction

1.1.1 Overview

Terminal Access Controller Access Control System (TACACS) is a distributed authentication, authorization and accounting (AAA) protocol based on the client/server architecture. TACACS+ has enhanced functions on the basis of the TACACS protocol, to provide the authentication, authorization and accounting services for users. This following describes TACACS+.

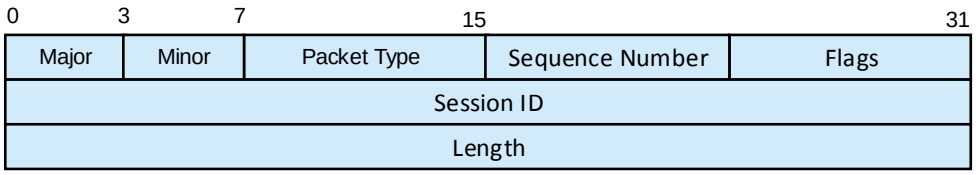
Both TACACS+ and Remote Authentication Dial-In User Service (RADIUS) are capable of providing AAA security services. Compared with RADIUS, TACACS+ has the following advantages:

- It is implemented based on the Transmission Control Protocol (TCP) and provides more reliable network transmission.
- TACACS+ encrypts both packet bodies and passwords to boost security.
- Authentication is separated from authorization. The authentication server and authorization server can be deployed separately in remote deployment.
- TACACS+ supports authorization and accounting on configuration commands.

1.1.2 Principles

1. TACACS+ Packet

Figure 1-1 TACACS+ Packet Structure



Fields contained in the TACACS+ packet structure shown in Figure 1-1 are described in Table 1-1.

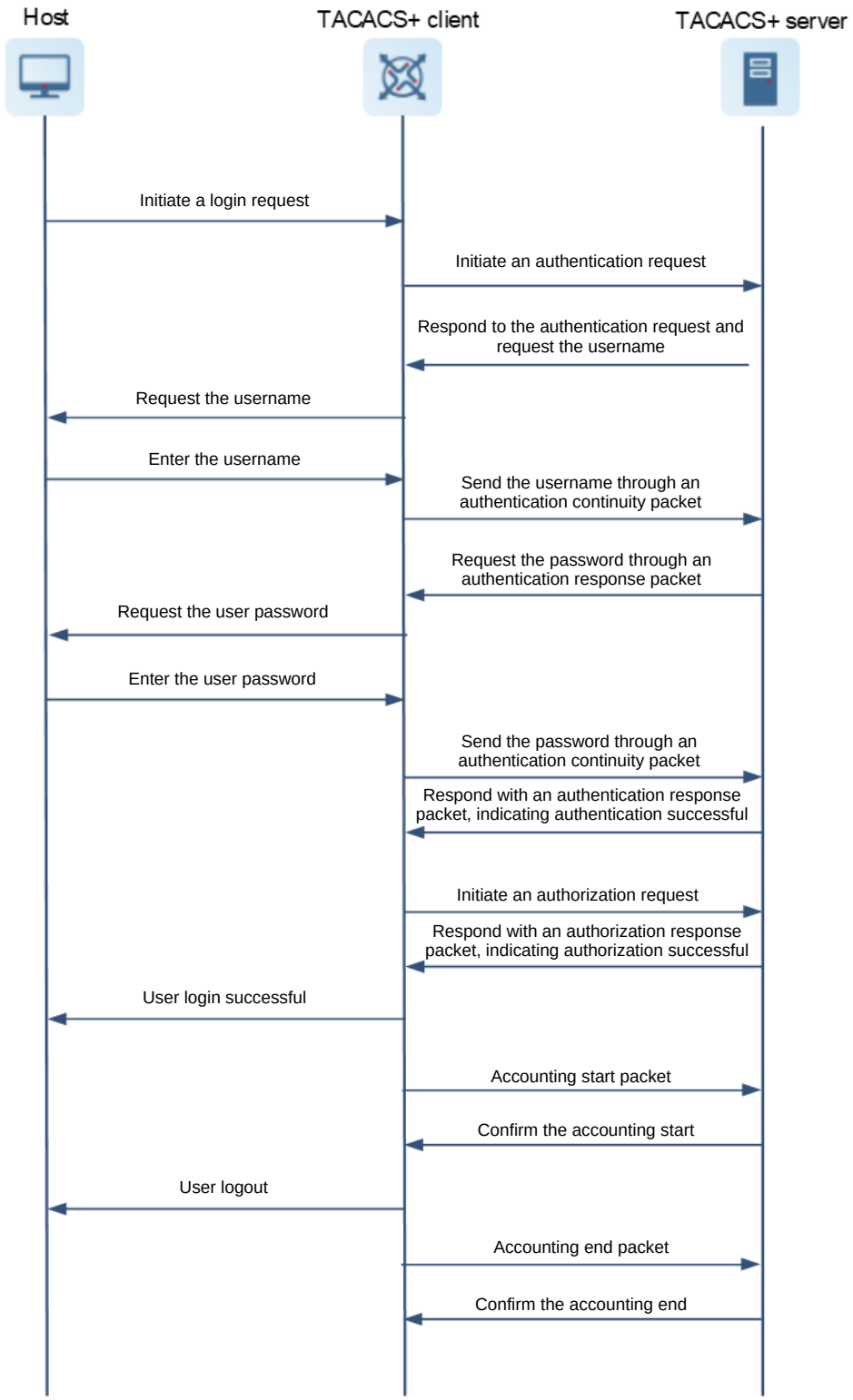
Table 1-1 Description of Fields Contained in a TACACS+ Packet

Field	Length	Description
Major Version	4 bits	Major TACACS+ version
Minor Version	4 bits	Minor TACACS+ version
Packet Type	1 byte	Packet type. The options are as follows: **0x01**: Indicates an authentication packet. **0x02**: Indicates an authorization packet. **0x03**: Indicates an accounting packet.

Field	Length	Description
Sequence Number	1 byte	Sequence number of a data packet in the current session (The sequence number of the first TACACS+ data packet in a session must be 1 and the sequence number of each subsequent data packet increases by one. The client sends data packets only with an odd sequence number and TACACS+ Daemon sends data packets only with an even sequence number.)
Flags	1 byte	Whether the data packet is encrypted
Session ID	4 bytes	TACACS+ session ID
Length	4 bytes	Body length of a TACACS+ data packet (excluding the header)

2. Packet Exchange Process

Figure 1-2 TACACS+ Packet Exchange Flowchart



As shown in Figure 1-2, the TACACS+ protocol basically involves the authentication, authorization, and accounting processes. The network access server (NAS) requests security services from the TACACS+ server as a TACACS+ client.

(1) Authentication process

a A user initiates a login request to the NAS.

b After receiving the user request, the NAS sends an authentication start packet to the TACACS+ server to initiate an authentication request.

c The TACACS+ server responds to the authentication request and asks the NAS to provide the username.

d The NAS asks the user terminal to provide the username.

e The user enters the username and sends it to the NAS.

f The NAS sends the username to the TACACS+ server through an authentication continuity packet.

g After receiving the username, the TACACS+ server continues to ask the NAS for the user password.

h The NAS requests the user terminal to provide the password.

i The user enters the password and sends it to the NAS.

j The NAS sends the password to the TACACS+ server through an authentication continuity packet.

k After receiving the password, the TACACS+ server verifies the password and then returns an authentication success message to the NAS.

(2) Authorization process

a The NAS initiates an authorization request to the TACACS+ server.

b The TACACS+ server responds to the authorization request by returning an authorization success message to the NAS.

c After receiving the authorization success message, the NAS allows the user to log in to the NAS and perform operations within the authorized scope.

(3) Accounting process

a The NAS sends an accounting start request to the TACACS+ server.

b After receiving the accounting start request, the TACACS+ server starts accounting and returns an accounting request acceptance message to the NAS.

c If the user logs out, the NAS sends an accounting end request to the TACACS+ server after receiving a user logout message.

d After receiving the accounting end request, the TACACS+ stops accounting and returns an accounting end message.

1.1.3 Protocols and Standards

- RFC 1492: Terminal Access Controller Access Control System

1.2 Configuration Task Summary

TACACS+ configuration includes the following tasks:

- Configuring TACACS+ Basic Features
- (Optional) Configuring TACACS+ Reachability Detection
- (Optional) Configuring a TACACS+ Server Group

1.3 Configuring TACACS+ Basic Features

1.3.1 Overview

This section describes how to configure parameters for the communication between the device and a TACACS+ server to ensure normal communication between them. After the parameters are configured, the device can correctly send AAA authentication, authorization, and accounting requests to the TACACS+ server and give responses.

1.3.2 Restrictions and Guidelines

Configuring TACACS+ basic features only ensures proper communication between the device and a TACACS+ server. To provide AAA security services for users, you still need to reference the TACACS+ server in an AAA method list.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA.

aaa new-model

(4) Configure a TACACS+ server.

tacacs-server host [**oob** [**via Mgmt** *Mgmt-number*]] { *ipv4-address* | *ipv6-address* } [**port** *port-number*] [**test username** *username*] [**idle-time** *idle-time*] [**timeout** *timeout*] [**key** [**0** | **7**] *key*]

No TACACS+ server is configured by default.

You can specify a shared key for a TACACS+ server when configuring the server. If it is not specified, the global shared key will be used.

(5) (Optional) Configure the global shared key for the communication between the device and TACACS+ server.

tacacs-server key [**0** | **7**] *key*

No global shared key is configured for the device and TACACS+ server by default.

(6) (Optional) Configure the source address for TACACS+ packets.

ip tacacs source-interface *interface-type interface-number*

No source address is configured for TACACS+ packets and the address is set by the network layer by default.

You can run this command to specify an outbound interface for packets. After this command is configured, the first IP address of the interface is used as the source address of TACACS+ packets.

(7) (Optional) Configure the timeout duration for the TACACS+ server.

tacacs-server timeout *timeout*

The default timeout duration of a TACACS+ server is **5** seconds in the communication between the device and the TACACS+ server.

1.4 Configuring TACACS+ Reachability Detection

1.4.1 Overview

A TACACS+ server can be only in the reachable or unreachable state. The device will not send authentication, authorization, or accounting requests of access users to an unreachable TACACS+ server unless all servers in the TACACS+ server group are unreachable.

The device maintains the reachability status of each TACACS+ server. The device selects a reachable TACACS+ server preferentially to improve the handling performance of TACACS+ services.

The device actively detects whether a specified TACACS+ server is reachable. After the active detection function is configured for a TACACS+ server, the device periodically sends detection requests (authentication requests or accounting requests) to the TACACS+ server. The active detection interval is **60** minutes when the TACACS+ server is reachable and **1** minute when the TACACS+ server is unreachable.

1.4.2 Restrictions and Guidelines

- To enable active detection for a specified TACACS+ server, perform the following configuration when configuring the TACACS+ server:
  - Configure a test username for the TACACS+ server.
  - Configure at least one tested port (authentication port or accounting port) for the TACACS+ server.
- It is judged that a TACACS+ server is unreachable only when both conditions below are met:
  - The device fails to receive a correct response packet from the TACACS+ server within the specified timeout period.
  - The consecutive transmission count of a request packet sent by the device to the same TACACS+ server reaches the specified timeout count.
- If any of the following conditions is met for an unreachable TACACS+ server, the TACACS+ server is considered reachable:
  - The device receives a correct response from the TACACS+ server.
  - The duration in which the TACACS+ server is unreachable exceeds the time configured using the **tacacs-server deadtime** command and active detection is disabled for the TACACS+ server.
  - The authentication port or accounting port of the TACACS+ server is updated on the device.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the criteria for the device to judge that a TACACS+ server is unreachable.

tacacs-server dead-criteria { **time** *timeout* **tries** *tries-number* | **time** *timeout* | **tries** *tries-number* }

The criteria for the device to judge that a TACACS+ server is unreachable are that the server timeout duration is **60** seconds and the consecutive timeout count is **10** by default.

(4) (Optional) Configure the duration for the device to stop sending request packets to an unreachable TACACS+ server.

tacacs-server deadtime *deadtime*

Even if a TACACS+ server is unreachable, the device still sends requests to the TACACS+ server by default.

If active detection is enabled for a TACACS+ server, the time parameter configured by the **tacacs-server deadtime** command does not take effect on the TACACS+ server.

1.5 Configuring a TACACS+ Server Group

1.5.1 Overview

One or more TACACS+ servers can be added to each TACACS+ server group, which provides AAA services for users as a whole.

1.5.2 Restrictions and Guidelines

- TACACS+ security services are a type of AAA services and need to be used in combination with the AAA features. TACACS+ provides security services for users as one method in an AAA method list.
- When configuring the authentication, authorization, and accounting method lists, you can specify server groups separately for them.
- In a user-defined server group, you can only specify and apply servers in the default server group.
- TACACS+ server groups support virtual routing and forwarding (VRF) instances. When a server group in a specified VRF instance is used, the source address used by the device to communicate with a remote server must be obtained from the VRF instance. If you run the **ip tacacs+ source-interface** command to specify the source interface for request packets, the IP address obtained from this source interface takes priority over that found in the VRF instance.
- The name of a server group cannot be set to the predefined keyword **tacacs+**.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a TACACS+ server group.

aaa group server tacacs+ *group-name*

No TACACS+ server group is configured by default.

You can group TACACS+ servers so that authentication, authorization, and accounting can be completed by different server groups.

(4) Add a server to the TACACS+ server group.

server { *ipv4-address* | *ipv6-address* }

No server is added to a TACACS+ server group by default.

(5) (Optional) Specify a VRF instance for the TACACS+ server group.

ip vrf forwarding *vrf-name*

No VRF instance is specified for a TACACS+ server group by default.

The VRF instance configured for a TACACS+ server group must use a valid name configured using the **vrf definition** command in global configuration mode.

(6) Configure an MGMT port to be used by the TACACS+ server group.

ip oob [**via Mgmt** *mgmt-number*]

No MGMT port to be used by a TACACS+ server group is configured by default.

(7) (Optional) Configure the function of carrying the **nas-ip** attribute in packets.

nas-ip { *ipv4-address* | *ipv6-address* }

Packets do not carry the **nas-ip** attribute by default.

1.6 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** commands to output debugging information.

Notice

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2 TACACS+ Monitoring

Command	Purpose
show tacacs	Displays the interaction between the device and each TACACS+ server.
debug tacacs+	Debugs TACACS+.

1.7 Configuration Examples

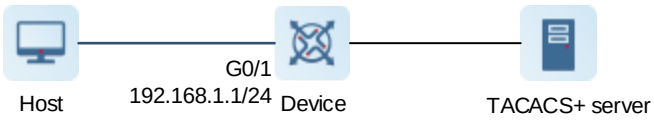
1.7.1 Configuring TACACS+ for Login Authentication

1. Requirements

A TACACS+ server needs to be used for authentication of login users.

2. Topology

Figure 1-3 Topology of Login Authentication Using TACACS+



3. Notes

- Configure device information and add login users on the TACACS+ server.
- Enable AAA security services on the device.
- Configure TACACS+ server information on the device.
- Configure a TACACS+ authentication method list.
- Apply the TACACS+ authentication methods to a specific line.

4. Procedure

(1) Configure device information and add login users on the TACACS+ server. The configuration is omitted here. For details, see the TACACS+ server configuration manual.

(2) Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

(3) Configure a TACACS+ server (the IP address of the TACACS+ server is set to 192.168.1.3 and the shared key is set to **sharekey** here).

```
Device(config)# tacacs-server host 192.168.1.3 key sharekey
```

(4) Configures an authentication method list.

```
Device(config)# aaa authentication login tacacs-method group tacacs+
```

(5) Apply the authentication methods to a line.

```
Device(config)# line vty 0 4
Device(config-line)# login authentication tacacs-method
```

5. Verification

After entering the correct username and password, a user can log in to the device successfully.

```
User Access Verification

Username:hostname1
Password:password1



Device#
```

6. Configuration Files

```
!
aaa new-model
!
aaa authentication login tacacs-method group tacacs+
!
tacacs-server host 192.168.1.3 key 7 $10$275$g8oXDDIPVeA=$
!
line console 0
```

```
line vty 0 4
 login authentication tacacs-method
!
```

7. Common Errors

The shared key configured on the device is inconsistent with that used by the TACACS+ server.

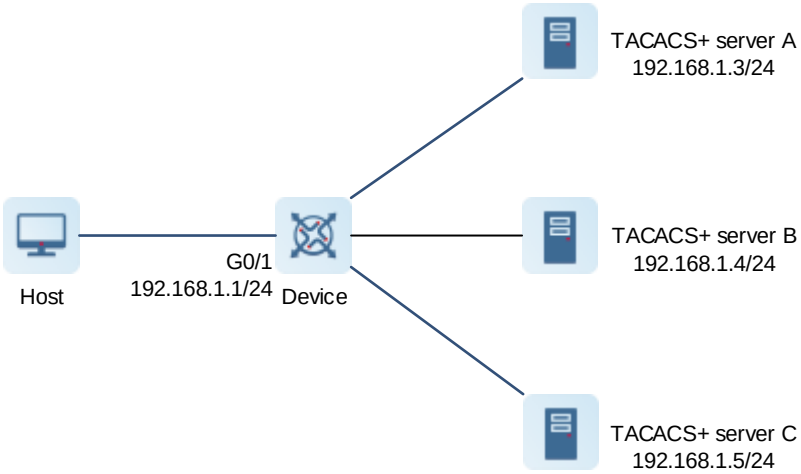
1.7.2 Configuring Separated Authentication, Authorization and Accounting by Using TACACS+

1. Requirements

The user authentication, authorization, and accounting services need to be separately completed by different TACACS+ server groups.

2. Topology

Figure 1-4 Topology of Separated Authentication, Authorization, and Accounting of TACACS+



3. Notes

- Configure device information and add login users on the TACACS+ server.
- Enable AAA security services on the device.
- Configure TACACS+ servers on the device and add them to different TACACS+ server groups.
- Configure TACACS+ authentication, authorization, and accounting method lists.
- Apply the TACACS+ authentication, authorization, and accounting methods to a specific line.

4. Procedure

(1) Configure device information and add login users on the TACACS+ server. The configuration is omitted here. For details, see the TACACS+ server configuration manual.

(2) Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

(3) Configure TACACS+ server A and add it to TACACS+ server group **tacacs1**. (The IP address of TACACS+ server A is set to 192.168.1.3 and the shared key is set to **sharekey** here.)

```
Device(config)# tacacs-server host 192.168.1.3 key sharekey
Device(config)# aaa group server tacacs+ tacacs1
Device(config-gs-tacacs+)# server 192.168.1.3
Device(config-gs-tacacs+)# exit
```

(4) Configure server groups **tacacs2** and **tacacs3** by referring to the steps of configuring server group **tacacs1**.

```
Device(config)# tacacs-server host 192.168.1.4 key sharekey
Device(config)# aaa group server tacacs+ tacacs2
Device(config-gs-tacacs+)# server 192.168.1.4
Device(config-gs-tacacs+)# exit
Device(config)# tacacs-server host 192.168.1.5 key sharekey
Device(config)# aaa group server tacacs+ tacacs3
Device(config-gs-tacacs+)# server 192.168.1.5
Device(config-gs-tacacs+)# exit
```

(5) Configure an authentication method list to use server group **tacacs1**, an authorization method list to use server group **tacacs2**, and an accounting method list to use server group **tacacs3**.

```
Device(config)# aaa authentication login tacacs-method group tacacs1
Device(config)# aaa authorization exec radius-method group tacacs2
Device(config)# aaa accounting exec radius-method start-stop group tacacs3
```

(6) Apply the authentication methods, authorization methods, and accounting methods to a line.

```
Device(config)# line vty 0 4
Device(config-line)# login authentication tacacs1
Device(config-line)# authorization exec tacacs2
Device(config-line)# accounting exec tacacs3
```

5. Verification

After entering the correct username and password configured on TACACS+ server A, a user can log in to the device successfully.

```
User Access Verification

Username:hostname1
Password:password1



Device#
```

After login, the user has only the privilege level granted by TACACS+ server B and can only run commands under this privilege level.

After the user logs out, accounting information of the user can be queried on TACACS+ server C. For details about how to query accounting information, see the TACACS+ server configuration manual.

6. Configuration Files

```
!
aaa new-model
```

```
!
aaa accounting exec radius-method start-stop group tacacs3
aaa authorization exec radius-method group tacacs2
aaa authentication login radius-method group tacacs1
!
tacacs-server host 192.168.1.3 key 7 $10$275$g8oXDDIPVeA=$
tacacs-server host 192.168.1.4 key 7 $10$275$g8oXDDIPVeA=$
tacacs-server host 192.168.1.5 key 7 $10$275$g8oXDDIPVeA=$
!
!
aaa group server tacacs+ tacacs1
 server 192.168.1.3
!
aaa group server tacacs+ tacacs2
 server 192.168.1.4
!
aaa group server tacacs+ tacacs3
 server 192.168.1.5
!
line console 0
line vty 0 4
 accounting exec tacacs3
 authorization exec tacacs2
 login authentication tacacs1
!
```

7. Common Errors

- The shared key configured on the device is inconsistent with that used by the TACACS+ server.
- Undefined servers are added to a server group.

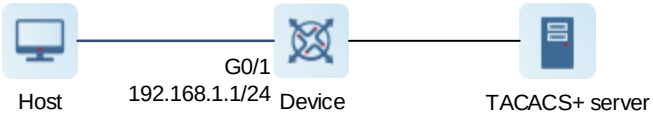
1.7.3 Configuring Reachability Detection

1. Requirements

TACACS+ reachability detection needs to be configured to identify unreachable TACACS+ servers.

1. Topology

Figure 1-5 Topology of TACACS+ Reachability Detection



2. Notes

- Configure the global criteria for judging that a TACACS+ server is unreachable.
- Configure an IP address for the TACACS+ server and configure active detection parameters.

3. Procedure

Configure the global criteria for judging that a TACACS+ server is unreachable as follows: The consecutive timeout count is **5** and the timeout duration is **120** seconds.

```
Device> enable
Device# configure terminal
Device(config)# radius-server dead-criteria time 120 tries 5
```

Set the IP address of the TACACS+ server to 192.168.1.3, detection username to **test**, detection interval to **90** minutes.

```
Device(config)# tacacs-server host 192.168.1.3 test username test idle-time 90
```

4. Verification

Disconnect the network communication between the device and the server with the IP address 192.168.1.3. Initiate TACACS+ authentication through the device. After 120 seconds, run the **show tacacs** command to check that the server status is "Dead".

```
Hostname# enable
Hostname# show tacacs server
Tacacs+ Server : 192.168.1.3/49
state: Dead
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 1

Tacacs capability:
   mgmt enable: true
   vrf enable: true
```

5. Configuration Files

```
!
tacacs-server host 192.168.1.3 test username test idle-time 90
tacacs-server dead-criteria time 120 tries 5
!
```

Contents

1 Configuring IEEE 802.1X 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 7
1.2 Configuration Task Summary 7
1.3 Configuring IEEE 802.1X Basic Features 8
1.3.1 Overview 8
1.3.2 Restrictions and Guidelines 9
1.3.3 Prerequisites 9
1.3.4 Procedure 9
1.4 Configuring IEEE 802.1X Parameters 10
1.4.1 Overview 10
1.4.2 Configuration Tasks 10
1.4.3 Configuring Re-authentication 11
1.4.4 Configuring Packet Retransmission Parameters 11
1.4.5 Configuring the Server Timeout Duration 12
1.4.6 Configuring the Quiet Period After an Authentication Failure 12
1.4.7 Configuring the Authentication Mode 13
1.4.8 Configuring Ruijie Client Detection 13
1.5 Configuring Authorization 14
1.5.1 Overview 14
1.5.2 Restrictions and Guidelines 14

1.5.3 Procedure....14

1.6 Configuring MAB....15

1.6.1 Overview....15

1.6.2 Restrictions and Guidelines....15

1.6.3 Configuration Tasks....15

1.6.4 Configuring Single-User MAB....16

1.6.5 Configuring Multi-User MAB....16

1.7 Configuring MAB Parameters....17

1.7.1 Overview....17

1.7.2 Configuration Tasks....17

1.7.3 Configuring the Username Format for MAB....18

1.7.4 Configuring the Username Uppercase/Lowercase for MAB....18

1.7.5 Configuring MAB VLAN....18

1.7.6 Configuring the MAB Timeout Duration....19

1.8 Configuring IAB....19

1.8.1 Overview....19

1.8.2 Restrictions and Guidelines....19

1.8.3 Procedure....20

1.9 Configuring the Port Control Mode....20

1.9.1 Overview....20

1.9.2 Configuration Tasks....20

1.9.3 Configuring the MAC-based Control Mode....21

1.9.4 Configuring the Port-based Control Mode....21

1.10 Configuring Automatic Dynamic VLAN Redirection on IEEE 802.1X Ports....22

1.10.1 Overview 22

1.10.2 Restrictions and Guidelines 22

1.10.3 Procedure 24

1.11 Configuring the Guest VLAN Function 24

1.11.1 Overview 24

1.11.2 Restrictions and Guidelines 24

1.11.3 Procedure 25

1.12 Configuring the Failed VLAN Function 25

1.12.1 Overview 25

1.12.2 Restrictions and Guidelines 25

1.12.3 Procedure 26

1.13 Configuring Extended Features 26

1.13.1 Overview 26

1.13.2 Configuration Tasks 26

1.13.3 Enabling Active Authentication 26

1.13.4 Configuring a List of Hosts Allowed for Authentication 27

1.13.5 Disabling the Virtual Source MAC Address Function 28

1.13.6 Configuring Multi-Account Authentication with One MAC Address 28

1.13.7 Configuring the Maximum Number of Users Who Can Be Authenticated on an Interface 28

1.13.8 Configuring the Function of Initiating Accounting After an IP Address Is Obtained 29

1.13.9 Configuring the Priority Order of IEEE 802.1X and MAB 29

1.13.10 Configuring the Accounting Update Period 30

1.13.11 Configuring Compatibility with H3C Clients and Servers 30

1.13.12 Disabling the Global IEEE 802.1X Features 31

1.14 Monitoring 31

1.15 Configuration Examples..... 33

1.15.1 Configuring IEEE 802.1X Authentication 33

1.15.2 Configuring the IP Authorization Mode 35

1.15.3 Configuring Multi-user MAB 36

1.15.4 Configuring IAB 37

1.15.5 Configuring Automatic Dynamic VLAN Redirection 39

1.15.6 Configuring Guest VLAN 40

1.15.7 Configuring Failed VLAN 41

1 Configuring IEEE 802.1X

1.1 Introduction

1.1.1 Overview

In a local area network (LAN) in compliance with the Institute of Electrical and Electronics Engineers (IEEE) 802 standards, users can connect to network devices to access network resources without authentication and authorization. This access mode does not pose obvious security problems in the early enterprise network application environment. However, with the large-scale development of applications such as mobile office and customer premises network (CPN) operation, this uncontrolled behavior brings great security risks. For this, IEEE develops the 802.1X protocol to solve LAN security problems.

IEEE 802.1X is a port-based network access control standard used to provide secure access services for LANs. This protocol complies with the authentication, authorization and accounting (AAA) security management mechanism. It is usually deployed on user access networks to provide port-based user AAA functions for network administrators.

1.1.2 Principles

1. Basic Concepts

- User

  Users usually refer to clients that need to access network resources. In an IEEE 802.1X wired environment, the MAC address and VLAN ID attributes of each user are unique for user differentiation. All other information (such as the account number and IP address) is changeable for users.

- RADIUS

  Remote Authentication Dial In User Service (RADIUS) is a remote authentication protocol applied widely to send authentication information between network devices and RADIUS servers. In actual IEEE 802.1X deployment, this protocol can be used to remotely deploy authentication servers.

- Timeout

  Timeout occurs when a device does not receive any response from a client or server within a specified period of time.

  The device needs to exchange packets with clients and servers during authentication. In response to unexpected factors such as network unavailability, a protocol sets the timeout duration for each exchange step. Each role needs to respond within the timeout duration during authentication. Otherwise, an authentication failure may be caused.

- EAP

  Extensible Authentication Protocol (EAP) carries IEEE 802.1X authentication information.

  EAP provides a universal authentication framework, which supports multiple authentication methods, such as the message digest 5 (MD5) authentication, Challenge-Handshake Authentication Protocol (CHAP) authentication, Password Authentication Protocol (PAP) authentication, and Transport Layer Security (TLS) authentication. Ruijie IEEE 802.1X module supports the MD5, CHAP, PAP, Protected Extensible

Authentication Protocol with Microsoft Challenge Handshake Authentication Protocol (PEAP-MSCHAP), and TLS authentication methods.

- EAPOL

  EAP over LAN (EAPOL) is the encapsulation of EAP on a LAN.

  EAPOL encapsulates packets based on the media access control (MAC) layer. The type number is 0x888E. The IEEE 802.1X standard assigns a multicast MAC address 01-80-C2-00-00-03 to the protocol to send packets in the initial authentication process. Ruijie authentication clients may use 01-D0-F8-00-00-03 as the multicast destination address at the beginning of authentication.

- EAPOR

  EAP over RADIUS (EAPOR) is the encapsulation of EAP over RADIUS.

  EAP packets are relayed by network devices. A network device encapsulates EAP packets into RADIUS packets over EAPOR and sends the packets to a RADIUS server for authentication.

2. Authentication

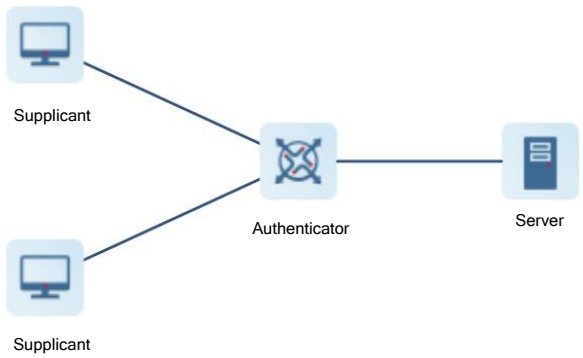
Authentication is a process of verifying user identities and determining whether a user has the legitimate permission to access network resources.

The basic principles of IEEE 802.1X authentication are as follows: A user submits the account and password to an authentication server through a network access server (NAS). The authentication server verifies the account and password. Only users who pass the authentication can obtain network access permissions.

- Authentication roles

  An IEEE 802.1X standard authentication system consists of three roles: supplicant, authenticator, and server, which correspond to the client, NAS, and authentication server (usually RADIUS server) in actual application.

Figure 1-1 Authentication Roles



  - Supplicant

    A supplicant is an end user who requests to access network resources. A supplicant is usually a PC.

    A supplicant needs to submit information used for authentication to an authenticator and respond to requests from the authenticator. According to the IEEE 802.1X protocol, a supplicant must run software in compliance with the IEEE 802.1X client standard and the software is responsible for submitting the account and password during authentication. The most typical software is the IEEE 802.1X client embedded in the operating system (OS). You can also use client software developed by vendors such as Ruijie RG Supplicant.

  - Authenticator

An authenticator is a NAS that manages supplicants' authentication status and network connection status.

An authenticator acts as an intermediary between a supplicant and an authentication server. It obtains the account and password used for authentication from a supplicant, and sends them to an authentication server. The authenticator also obtains authentication-related information from the authentication server and sends the information to the supplicant.

- Authentication server

  An authentication server provides the authentication service for users. An authentication server is usually a RADIUS server.

  An authentication server stores legitimate user information and users' authorization information. It checks whether a user is legitimate by verifying the account and password submitted by a supplicant, and manages accounting data submitted by an authenticator. One authentication server can provide the authentication service for multiple supplicants to implement centralized management of users.

- Port type

  There are two types of ports on the device that serves as an authenticator: controlled port and uncontrolled port.

  Users connected to a controlled port can access network resources only after passing authentication. Otherwise, the users can only transmit packets used for authentication. Users connected to an uncontrolled port can access network resources without authentication. The access to network resources needs to be controlled for supplicants and therefore, supplicants need to be connected to controlled ports. Network permission control is not required for authentication servers, and therefore, they need to be connected to uncontrolled ports.

- Authentication process

  A supplicant and an authenticator exchange information through the EAPOL protocol, and an authenticator and an authentication server exchange information through the EAPOR protocol.

  The figure below shows a typical IEEE 802.1X authentication process.

Figure 1-2 Authentication Packet Exchange

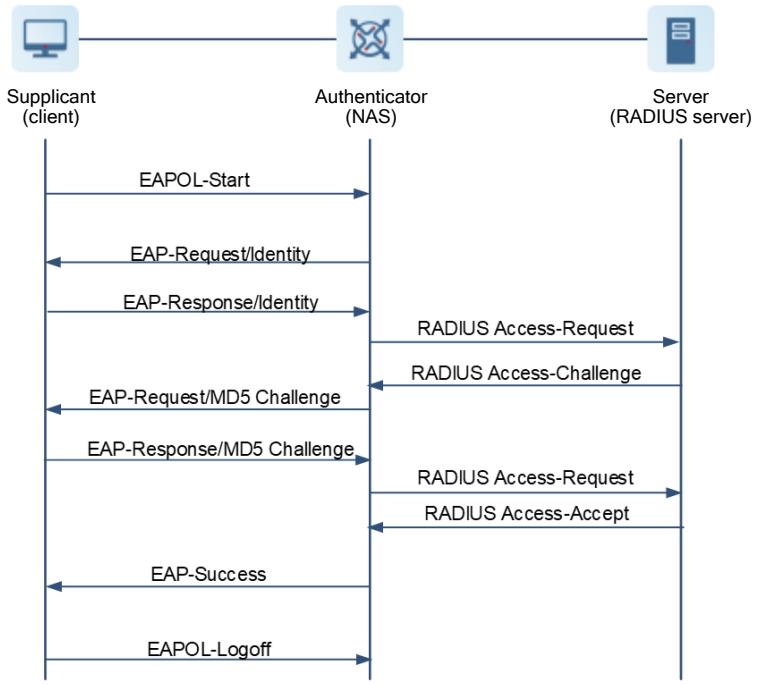


Figure 1-2 shows a typical user-initiated authentication process.

a A user starts the IEEE 802.1X client application on a client and enters the account and password. The client initiates an authentication request to a NAS. So the client sends an authentication request frame (EAPOL-Start) to the NAS.

b After receiving the frame, the NAS sends an EAP request frame of the identity type (EAP-Request/Identity) to the client, asking the client to provide the account for authentication.

c After receiving the request frame from the NAS, the client sends the account to the NAS through a response frame of the identity type (EAP-Response/Identity).

d After receiving the response frame from the client, the NAS retrieves the EAP packet from the frame, encapsulates the EAP packet into a RADIUS packet (RADIUS Access-Request), and sends the packet to an authentication server for processing.

e After receiving the Access-Request packet from the NAS, the authentication server parses the account and encrypts the password corresponding to the username by using a randomly generated MD5 Challenge to obtain the encrypted password. The authentication server sends the MD5 Challenge to the NAS through a RADIUS Access-Request packet.

f The NAS forwards the MD5 Challenge sent by the RADIUS server to the client.

g The client encrypts the local password by using the received MD5 Challenge and sends the encrypted password to the NAS through an EAP-Response/MD5 packet.

h The NAS encapsulates the received EAP-Response/MD5 packets into a RADIUS Access-Request packet and sends the packet to the authentication server.

i The authentication server retrieves the encrypted password from the RADIUS Access-Request packet and compares it with the encrypted password obtained in step e. If they are the same, the authentication server considers the user legitimate and returns an authentication success packet (RADIUS access-Accept) to the NAS.

j After receiving the packet, the NAS sends an authentication success frame (EAP-Success) to the client, changes the port status to the authorized state, and allows the user to access the network through the port.

In some special cases (for example, authentication is performed immediately when a user connects to a network), the NAS may actively initiate an authentication request and the step that a user actively initiates a request is skipped.

- User status during authentication

  All users connected to uncontrolled ports can use network resources. Whether users connected to controlled ports can access network resources depends on their authentication status. A user connected to a controlled port cannot access the network when just initiating authentication, and the user is in the unauthorized state. After passing authentication, the user can access the network normally and the status changes to authorized.

  On an IEEE 802.1X-supported network device, all ports are uncontrolled ports by default. You can configure a port as a controlled port to enable all users connected to the port to pass authentication before accessing the network.

  Common user authentication states and behaviors are described as follows:

  - If a user is still in the unauthorized state due to an authentication failure, the user can initiate authentication again.
  - If the network between the NAS and the authentication server is unreachable, a user connected to the NAS is in the unauthorized state.
  - After a user sends an EAPOL-LOGOFF packet, the user transitions from the authorized state to the unauthorized state.
  - When a port on an NAS changes to the LINK-DOWN state, all users connected to the port transition to the unauthorized state.
  - When the NAS is restarted, all users served by the NAS transitions to the unauthorized state.
  - If a client does not support IEEE 802.1X and is connected to a controlled port, the client cannot respond to requests from the NAS and cannot complete authentication. The client is always in the unauthorized state and cannot access network resources.
  - If a client supports IEEE 802.1X but the NAS does not, the NAS does not respond to the EAPOL-Start frame from the client. If the client still receives no response after sending a certain number of EAPOL-Start frames, the client considers the access port as an uncontrolled port and accesses network resources directly.

- Deploying an authentication server

  Ruijie IEEE 802.1X module is compatible with RADIUS servers. RADIUS servers can be used for environment deployment, such as Ruijie SAM/SMP, Microsoft IAS/NPS, and Cisco ACS and Free RADIUS Server. For deployment steps, see the server operation manual.

- Configuring authentication parameters

  To make IEEE 802.1X on an NAS take effect, complete the following configuration:

  a Configure RADIUS server parameters to ensure the network between the NAS and the RADIUS server is reachable.

  b Ensure that the server timeout duration of IEEE 802.1X is greater than that of RADIUS.

  c Configure and apply an AAA method list.

d Enable IEEE 802.1X authentication on the access port.

- Supplicant

  A supplicant refers to IEEE 802.1X-compliant client software installed on a terminal. A user can start the Supplicant software on a terminal and enter the account to initiate authentication.

  If a terminal uses the client embedded in the OS, when the network is available, the terminal automatically displays a dialog box, asking you to enter the account and password for authentication. The implementation and UI operation methods of different client software may be different. You are advised to use Ruijie Supplicant software as the authentication client. If you use other software, see relevant software instructions.

- Going offline

  When stopping accessing network resources, a user can go offline by shutting down the client, disconnecting the network, or logging out of Supplicant.

3. Authorization

Authorization refers to binding specified services to authenticated users, for example, binding an IP address, VLAN, access control list (ACL), quality of service (QoS), available Internet access time range, and available bandwidth. A user is identified by MAC address and VLAN ID (VID). Authorization is actually to add permission information on the basis of MAC address and VLAN ID, such as bound IP address and accessible VLANs.

- IP authorization

  The IEEE 802.1X authentication standard cannot identify IP information. Ruijie IEEE 802.1X module extends the application of IEEE 802.1X and supports MAC+IP binding, which is called IP authorization.

  IP authorization supports four modes:

  - Supplicant authorization: An IP address is provided by Supplicant and this authorization mode needs to be used in combination with Ruijie Supplicant.
  - RADIUS authorization: An IP address is delivered by a RADIUS server to the device after the authentication succeeds.
  - Dynamic Host Configuration Protocol (DHCP) authorization: An authenticated client initiates a DHCP request. After obtaining an IP address, the device binds the IP address with the client's MAC address. DHCP authorization applies to a dynamic IP address environment.
  - Mixed authorization: Authenticated clients select an IP authorization mode based on the sequence of Supplicant authorization, RADIUS authorization, and DHCP authorization, and then the device completes MAC+IP binding. That is, the IP address provided by Supplicant is preferentially used, followed by the IP address assigned by a RADIUS server. The IP address assigned by DHCP is used only when neither of the preceding two IP addresses exists.

- ACL authorization

  ACL authorization means that a server delivers specific ACL services to authenticated users.

  ACL authorization is delivered based on RADIUS attributes and supports standard attributes, Ruijie private attributes, and Cisco private attributes. For details, see the RADIUS server manual.

- Kicking users offline

  Kicking users offline is to force users to go offline. When Ruijie IEEE 802.1X module is used together with Ruijie SAM/SMP, servers can kick online users offline. Then, the users cannot access the network. This

function applies to scenarios, in which the Internet access time range needs to be controlled and Internet access charges need to be checked in real time.

4. Accounting

The accounting function is used to audit Internet access behaviors and charges of access users (including auditing the online duration and traffic).

To make the accounting function take effect, configure the accounting function on the device and ensure that the RADIUS server supports the accounting audit function defined in RFC2869.

When a user goes online, the device sends an accounting start packet to the server and the server starts accounting. When the user goes offline, the device sends an accounting end packet to the server, and the server completes an audit and generates an Internet access fee audit list.

Notice

The implementation of the accounting function may vary with servers and not all servers support the accounting function. Therefore, refer to the server usage instructions during actual deployment.

- Accounting start

  After a user passes authentication, the device sends an accounting start packet to the server. After receiving the packet, the server starts the accounting for the user.

  The accounting start packet carries accounting attributes of the user, such as the username and accounting ID.

- Accounting update

  The device periodically sends accounting update packets to the server, making the accounting on the server more real-time.

  The interval for sending accounting update packets can be configured on the device or delivered by the server.

- Accounting end

  After a user logs out, the device sends an accounting end packet to the server. The accounting end packet carries the online duration and traffic of the user. The server generates Internet access records based on the information.

1.1.3 Protocols and Standards

- IEEE802.1X: Port-Based Network Access Control
- RFC2869: RADIUS Extensions

1.2 Configuration Task Summary

IEEE 802.1X configuration includes the following tasks:

(1) Configuring IEEE 802.1X Basic Features

(2) (Optional) Configuring IEEE 802.1X Parameters. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring Re-authentication

- Configuring Packet Retransmission Parameters
- Configuring the Server Timeout Duration
- Configuring the Quiet Period After an Authentication Failure
- Configuring the Authentication Mode
- Configuring Ruijie Client Detection

(3) (Optional) Configuring Authorization

(4) (Optional) Configuring MAB. Select any of the following configuration tasks to configure.

- Configuring Single-User MAB
- Configuring Multi-User MAB

(5) (Optional) Configuring MAB Parameters. All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Username Format for MAB
- Configuring the Username Uppercase/Lowercase for MAB
- Configuring MAB VLAN
- Configuring the MAB Timeout Duration

(6) (Optional) Configuring IAB

(7) (Optional) Configuring the Port Control Mode

(8) (Optional) Configuring Automatic Dynamic VLAN Redirection on IEEE 802.1X Ports

(9) (Optional) Configuring the Guest VLAN Function

(10) (Optional) Configuring the Failed VLAN Function

(11) (Optional) Configuring Extended Features. All the configuration tasks below are optional. Select the configuration tasks as required.

- Enabling Active Authentication
- Configuring a List of Hosts Allowed for Authentication
- Disabling the Virtual Source MAC Address Function
- Configuring Multi-Account Authentication with One MAC Address
- Configuring the Maximum Number of Users Who Can Be Authenticated on an Interface
- Configuring the Function of Initiating Accounting After an IP Address Is Obtained
- Configuring the Priority Order of IEEE 802.1X and MAB
- Configuring the Accounting Update Period
- Configuring Compatibility with H3C Clients and Servers
- Disabling the Global IEEE 802.1X Features

1.3 Configuring IEEE 802.1X Basic Features

1.3.1 Overview

This section describes how to enable 802.1X features to provide basic authentication and accounting services.

1.3.2 Restrictions and Guidelines

- In interface configuration mode, you can enable/disable IEEE 802.1X authentication on the interface.
- Configure RADIUS parameters accurately to ensure that the basic RADIUS communication is proper. Configure an IP address and a protocol communication port for the authentication server as well as the encrypted key used for the communication between the NAS and the RADIUS server.
- The IEEE 802.1X authentication method list and accounting method list must be configured in AAA. Otherwise, an error may occur in authentication and accounting.
- IEEE 802.1X uses default method lists by default. To use other method lists, run the **dot1x authentication** and **dot1x accounting** commands to apply the method lists to be used by IEEE 802.1X.
- You can run the **aaa accounting update** command in global configuration mode to enable the accounting update function. The accounting update interval can be configured using the **aaa accounting update periodic** command or delivered by the server. If delivered by the server, the parameter configuration delivered by the server is used preferentially. If the server does not deliver the parameter configuration, the local configuration is used. For details about the accounting update function, see "Configuring AAA" in the *Security Configuration Guide*.
- If IEEE 802.1X is enabled on a port and the number of authenticated users exceeds the maximum number of users supported by port security, port security cannot be enabled. For details about port security, see "Configuring Port Security" in the *Security Configuration Guide*.
- When both port security and IEEE 802.1X are enabled, if the address of port security ages, IEEE 802.1X-authenticated users must be re-authenticated before making further communication.
- Users using static IP addresses or complying with IP+MAC binding can access the network without authentication.
- When Ruijie SAM/SMP software is used together, the accounting function must be configured. Otherwise, the server cannot perceive users going offline.

1.3.3 Prerequisites

Complete required configuration (such as account configuration) on the authentication server to ensure smooth authentication. For details, see the authentication server user manual.

1.3.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Create an IEEE 802.1X authentication method list and an accounting method list.

a Create an IEEE 802.1X authentication method list.

aaa authentication dot1x { **default** | *list-name* } { *method* }&<1-4>

No IEEE 802.1X authentication method list is configured by default.

b Create an IEEE 802.1X accounting method list.

aaa accounting network { **default** | *list-name* } **start-stop** { *method* }&<1-4>

No IEEE 802.1X accounting method list is configured by default.

(5) (Optional) Configure RADIUS server parameters.

This step is mandatory if the authentication and accounting methods use a RADIUS server.

a Configure a RADIUS server.

radius-server host [**oob** [**via Mgmt** *Mgmt_number*]] { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port-number* | **acct-port** *acct-port-number*] * [**test username** *username* [**ignore-acct-port**] [**ignore-auth-port**] [**idle-time** *idle-time*]] [**key** [**0** | **7**] *text-string*]

No RADIUS server is configured by default.

b Configure a shared key for the communication between the device and the RADIUS server.

radius-server key [**0** | **7**] *text-string*

No shared key for the communication between the device and a RADIUS server is configured by default.

(6) Apply the IEEE 802.1X authentication method list and accounting method list.

a Apply the IEEE 802.1X authentication method list.

dot1x authentication { **default** | *list-name* }

b Apply the IEEE 802.1X accounting method list.

dot1x accounting { **default |** *list-name* }

(7) Enter the interface configuration mode.

- Enter the interface configuration mode.

  interface *interface-type interface-number*

- Enter the batch interface configuration mode.

  interface range *interface-type slot-number/interface-number*

(8) Enable IEEE 802.1X authentication.

dot1x port-control auto

1.4 Configuring IEEE 802.1X Parameters

1.4.1 Overview

After IEEE 802.1X basic features are configured, you may need to adjust protocol parameter configuration based on the actual deployment and network status.

1.4.2 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring Re-authentication
- Configuring Packet Retransmission Parameters
- Configuring the Server Timeout Duration

- Configuring the Quiet Period After an Authentication Failure
- Configuring the Authentication Mode
- Configuring Ruijie Client Detection

1.4.3 Configuring Re-authentication

1. Overview

Re-authentication refers that a device periodically requests users to perform re-authentication.

Re-authentication prevents authenticated users from being pretended by other users, and detects whether they are offline, making the accounting more accurate.

2. Restrictions and Guidelines

- After re-authentication is enabled, the device can periodically re-authenticate online users. Re-authentication brings great burden to the server. You are advised to disable this function in the existence of considerable users.
- The re-authentication function can be enabled/disabled, and the re-authentication interval can be configured. In duration-based accounting scenarios, determine the re-authentication interval based on the network scale to ensure reasonable interval and accurate accounting.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable re-authentication.

dot1x re-authentication

The re-authentication function is disabled by default.

(4) (Optional) Configure the re-authentication interval.

dot1x timeout re-authperiod *interval*

The default re-authentication interval is **3600** seconds.

1.4.4 Configuring Packet Retransmission Parameters

1. Overview

A supplicant and an authenticator exchange packets during authentication. Packets need to be retransmitted due to abnormal causes such as timeout. You can configure the retransmission count, retransmission interval, and other parameters based on the actual network conditions.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure packet retransmission parameters. Configure at least one of the tasks.

- Configure the retransmission interval of Request/Identity packets.

  dot1x timeout tx-period *interval*

  The default retransmission interval of Request/Identity packets is **3** seconds.

- Configure the maximum retransmission count of Request/Identity packets.

  dot1x reauth-max *reauth-max-number*

  The default maximum retransmission count of Request/Identity packets is **3**.

- Configure the retransmission interval of Request/Challenge packets.

  dot1x timeout supp-timeout *interval*

  The default retransmission interval of Request/Challenge packets is **3** seconds.

- Configure the maximum retransmission count of Request/Challenge packets.

  dot1x max-req *max-req-number*

  The default maximum retransmission count of Request/Challenge packets is **3**.

1.4.5 Configuring the Server Timeout Duration

1. Overview

This section describes how to configure the server timeout duration of the IEEE 802.1X protocol.

2. Restrictions and Guidelines

- Both the IEEE 802.1X and RADIUS protocols have their own server timeout parameters. Ensure that the server timeout duration of IEEE 802.1X is greater than that of RADIUS. For details about the server timeout parameter of RADIUS, see "Configuring RADIUS" in the *Security Configuration Guide*.
- In an environment with poor server performance, you are advised to set the server timeout duration to a larger value.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the server timeout duration.

dot1x timeout server-timeout *server-timeout*

The default server timeout duration is **5** seconds.

1.4.6 Configuring the Quiet Period After an Authentication Failure

1. Overview

After the quiet period after an authentication failure is configured, a user who fails the authentication needs to wait for a period of time before initiating another authentication. The purpose is to prevent malicious users from conducting frequent authentication to crack passwords in a brute force manner or launch denial of service (DoS) attacks.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the quiet period after an authentication failure.

dot1x timeout quiet-period *quiet-period*

The default quiet period after an authentication failure is **10** seconds.

1.4.7 Configuring the Authentication Mode

1. Overview

Authentication servers and authentication clients may support different authentication modes. You need to select an appropriate authentication mode based on the authentication modes supported by authentication servers and clients. Currently, CHAP, EAP, and PAP authentication modes are supported.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the authentication mode.

dot1x auth-mode { **chap** | **eap** | **pap** }

The default authentication mode is EAP.

1.4.8 Configuring Ruijie Client Detection

1. Overview

This section describes how to configure Ruijie client detection to detect whether clients are online.

2. Restrictions and Guidelines

Ruijie client detection applies only to Ruijie clients. You are advised to enable this function when Ruijie clients are used.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable online Ruijie client detection.

dot1x client-probe enable

Online Ruijie client detection is disabled by default.

(4) (Optional) Configure Ruijie client detection parameters. Configure at least one of the tasks.

- Configure the Ruijie client detection interval.

dot1x probe-timer interval *interval*

The default client detection interval is **20** seconds.

- Configure the Ruijie client detection duration.

  dot1x probe-timer alive *alive-time*

  The default Ruijie client detection duration is **250** seconds.

1.5 Configuring Authorization

1.5.1 Overview

- IP authorization

  IP authorization aims to restrict authenticated users to using specified IP addresses to access the network, and prevent IP address embezzlement.

- Non-Ruijie client filtering

  This function aims to restrict clients to using Ruijie Supplicant for authentication, so as to obtain the anti-proxy, SMS, and other functions provided by Ruijie Supplicant.

- 2nd-generation Ruijie Supplicant deployment

  2nd-generation Ruijie Supplicant deployment means that a user downloads Ruijie Supplicant through the Web page and then initiates authentication by using Ruijie Supplicant. 2nd-generation Ruijie Supplicant deployment facilitates fast deployment of Ruijie Supplicant in an environment with massive users.

1.5.2 Restrictions and Guidelines

- If the function of kicking users offline in real time provided by Ruijie SAM/SMP software needs to be used, configure Simple Network Management Protocol (SNMP) parameters correctly. For the SNMP parameter configuration, see "Configuring SNMP" in the *Network Management and Monitoring Configuration Guide*.
- When multiple types of authentication client software are used in the network, disable the non-Ruijie client filtering function.
- Changing the IP authorization mode will force authenticated users offline and they need to be re-authenticated before going online again.
- In mixed authorization mode, if an IP authorization mode with a higher priority takes effect during user authentication, the IP authorization mode with a higher priority is used. If RADIUS authorization is used originally but Supplicant provides an IP address during re-authentication, this address is used for authorization.
- 2nd-generation Ruijie Supplicant deployment and Web authentication are mutually exclusive.
- Redirection parameters need to be configured for 2nd-generation Ruijie Supplicant deployment. For details about redirection parameters, see "Configuring Web Authentication" in the *Security Configuration Guide*.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the global IP authorization mode.

aaa authorization ip-auth-mode { **disable** | **supplicant** | **radius-server** | **dhcp-server** | **mixed** }

Global IP authorization is disabled by default.

(4) (Optional) Enable 2nd-generation Ruijie Supplicant deployment function.

dot1x redirect

The 2nd-generation Ruijie Supplicant deployment function is disabled by default.

After 2nd-generation Ruijie Supplicant deployment is configured, users who are connected to controlled ports and have no IEEE 802.1X client installed can download the IEEE 802.1X client through the Web page.

(5) (Optional) Enable the non-Ruijie client filtering function.

dot1x private-supplicant-only

The non-Ruijie client filtering function is disabled by default.

1.6 Configuring MAB

1.6.1 Overview

In actual environments, the IEEE 802.1X client cannot be installed on some dumb terminals (such as network printers). They cannot complete IEEE 802.1X authentication but their security needs to be controlled. In this case, you can configure the MAC authentication bypass (MAB) to complete the authentication of these dumb terminals.

MAB is an authentication method that uses MAC addresses of terminals as the usernames and passwords for authentication without installing the client. MAB is mainly used to provide network access control for some dumb terminals.

1.6.2 Restrictions and Guidelines

- The IEEE 802.1X function must be enabled on a controlled port before MAB is configured.
- A MAB-enabled port sends an authentication request packet at an interval specified by **tx-period**. If the request packet is sent for a certain number of times specified by **reauth-max** but no response is received from the client, the port enters the MAB mode. Ports in MAB mode can learn MAC addresses and use them as accounts for authentication.
- When configuring MAC accounts that are used as usernames and passwords on the authentication server, be sure to use the format without separators. For example, assume that the MAC address of a terminal is 00-d0-f8-00-01-02. The account added on the authentication server should be 00d0f8000102.
- IEEE 802.1X has a higher priority than MAB. If a MAB-authenticated terminal needs to go through IEEE 802.1X authentication, the device will clear MAB authentication information of the terminal.
- MAB supports only the PAP authentication mode. Ensure that MAB parameter configurations on the device are consistent with those on the authentication server.
- MAB checks whether terminals can complete IEEE 802.1X authentication by using active authentication. Therefore, enable active authentication when deploying MAB.

1.6.3 Configuration Tasks

Configure MAB. Select any of the following configuration tasks to configure.

- Configuring Single-User MAB

- Configuring Multi-User MAB

1.6.4 Configuring Single-User MAB

1. Overview

Single-user MAB applies to the scenario, in which a port has only one dumb terminal attached to it or a port has only one dumb terminal to be authenticated. After successful authentication, other terminals connected to the port can access the network.

2. Restrictions and Guidelines

As long as the MAC address of one terminal connected to a port passes MAB authentication, all terminals connected to the port are allowed to access the network. However, in some security applications, the administrator requires that only one MAC address exist under a single-user MAB port. In this case, you can configure MAB violation on this port. After MAB violation is configured on a port and the port enters the MAB mode, if more than one MAC address is found under the port, violation occurs on the port.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable single-user MAB.

dot1x mac-auth-bypass

Single-user MAB is disabled by default.

(5) (Optional) Enable MAB violation.

dot1x mac-auth-bypass violation

MAB violation is disabled by default.

1.6.5 Configuring Multi-User MAB

1. Overview

Multi-user MAB applies when multiple dumb terminals are connected to one port.

2. Restrictions and Guidelines

- Multi-user MAB can be used together with IEEE 802.1X authentication in mixed access scenarios such as the PC+VoIP daisy-chain topology.
- After multi-user MAB is enabled, illegitimate users connected to an interface may attack the device. Therefore, it is necessary to prevent illegitimate users from frequently initiating authentication, in an effort to reduce the server load. Configure the quiet period after a multi-user MAB failure in global configuration mode. After configuration, if a user fails the authentication, the user can re-initiate authentication only after the quiet period elapses. Configure this quiet period based on the network environment.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable multi-user MAB.

dot1x mac-auth-bypass multi-user

Multi-user MAB is disabled by default.

(5) (Optional) Configure the quiet period after a multi-user MAB failure.

dot1x multi-mab quiet-period *quiet-period*

The default quiet period after a multi-user MAB failure is **30** seconds.

You can use this command to restrict the authentication frequency of dumb terminals connected to a port.

(6) (Optional) Configure the number of authentication failures required for user entry aging.

dot1x multi-mab quiet-user fail-times [*fail-times*]

The default number of authentication failures required for user entry aging is **60**.

(7) (Optional) Configure the rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry.

dot1x multi-mab quiet-user authen-num [*authen-num*]

The default rate of initiating authentication using the MAC address in a multi-user MAB quiet user entry is **50** MAC addresses per second.

(8) (Optional) Configure the server rejection count for the device to delete a user entry.

dot1x multi-mab quiet-user reject-times [*reject-times*]

The default server rejection count for the device to delete a user entry is **1**.

1.7 Configuring MAB Parameters

1.7.1 Overview

This section describes how to configure MAB parameters to meet requirements of the authentication server for MAB.

1.7.2 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Username Format for MAB
- Configuring the Username Uppercase/Lowercase for MAB
- Configuring MAB VLAN
- Configuring the MAB Timeout Duration

1.7.3 Configuring the Username Format for MAB

1. Restrictions and Guidelines

The following four username formats are supported:

- **with-colon**: Indicates that the username format is xx:xx:xx:xx:xx:xx.
- **with-dot**: Indicates that the username format is xxxx.xxxx.xxxx.
- **with-hyphen**: Indicates that the username format is xx-xx-xx-xx-xx-xx.
- **with-3hyphen**: Indicates that the username format is xxxx-xxxx-xxxx.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the username format for MAB.

dot1x mab-username format [**with-colon** | **with-dot** | **with-hyphen** | **with-3hyphen**]

No username format for MAB is configured by default.

1.7.4 Configuring the Username Uppercase/Lowercase for MAB

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure usernames used for MAB to use uppercase letters.

dot1x mab-username upper

Usernames used for MAB use lowercase letters by default.

This command is used to meet requirements of different servers for username uppercase/lowercase in MAB.

1.7.5 Configuring MAB VLAN

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure MAB VLAN.

dot1x mac-auth-bypass vlan *vlan-id*

The MAB VLAN function is disabled by default.

If MAB is needed for users only in some VLANs of an interface, you can configure the VLANs as MAB VLANs. Users not in the MAB VLANs cannot perform MAB.

1.7.6 Configuring the MAB Timeout Duration

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the MAB timeout duration.

dot1x mac-auth-bypass timeout-activity *timeout*

MAB does not time out by default.

You can configure this parameter to restrict the network access duration of dumb terminals.

1.8 Configuring IAB

1.8.1 Overview

Inaccessible authentication bypass (IAB) is a method provided for new to-be-authenticated users to access the network when all RADIUS servers configured on the device are all unreachable. After a RADIUS server becomes reachable, it verifies the identities of users authorized in the unavailability period of RADIUS servers.

When RADIUS servers connected to a port are inaccessible and cannot authenticate the identities of users for the time being, you can add the port to a specified VLAN so that users connected to the port can access network resources only in the specified VLAN. This VLAN is called an IAB VLAN.

1.8.2 Restrictions and Guidelines

- IAB takes effect only when the global IEEE 802.1X authentication method list contains only the RADIUS authentication method and all RADIUS servers in the method list fail. If the method list has other authentication methods (such as local and none), IAB does not take effect.
- Configure an account for testing whether a RADIUS server is reachable and the criteria for judging that a RADIUS server is unreachable. For details about the criteria for judging that a RADIUS server is unreachable, see "Configuring RADIUS" in the *Security Configuration Guide*. After global multi-domain AAA is enabled, the global method list is not used during IEEE 802.1X authentication. When IAB configured on a port detects that all RADIUS servers configured in the global 802.1X authentication method list are inaccessible, it directly returns an authentication success message to users, who can access network resources with no need to enter usernames. In this case, multi-domain AAA does not take effect on this port.
- Users authenticated in IAB mode do not initiate accounting requests to the accounting server.
- Authenticated users can properly access the network and are not affected by server inaccessibility.
- In access authentication configuration mode, when 802.1X-based IP authentication is enabled globally, if a user connected to a port is authenticated, IAB cannot be performed on other users connected to the port. In gateway authentication mode, IP authorization can be performed only when IP addresses of authenticated

users can be obtained.

- Complete IEEE 802.1X authentication is required on some IEEE 802.1X authentication clients (such as Windows IEEE 802.1X authentication clients) so that ports connected to the clients are considered authenticated. When IAB is performed on such clients, users actually have been authorized via IAB but an authentication failure may be displayed on the clients.
- If an IAB VLAN does not exist, it is dynamically created when a port is added to the IAB VLAN, and automatically deleted when the port is removed from the IAB VLAN.
- An IAB VLAN cannot be a private VLAN, remote VLAN, or super VLAN (including sub VLANs).

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable IAB.

dot1x critical

IAB is disabled by default.

(5) (Optional) Enable IAB recovery.

dot1x critical recovery action reinitialize

IAB recovery is disabled by default.

After this function is enabled on a port, when a server becomes reachable, users who are connected to the port and normally authenticated can access the network without re-authentication. For those who are IAB-authenticated during server unavailability, the device initiates active authentication.

(6) (Optional) Configure the IAB VLAN function.

dot1x critical vlan *vlan-id*

The IAB VLAN function is disabled by default.

1.9 Configuring the Port Control Mode

1.9.1 Overview

IEEE 802.1X control is classified into MAC-based control and port-based control. The control granularity of the two control modes is different. Configure the control mode as required.

In MAC-based control mode, each client connected to a port must pass authentication before accessing network resources. In port-based control mode, all clients connected to a port can access network resources as long as one of them is authenticated. The MAC-based control mode is used by default.

1.9.2 Configuration Tasks

Configure the port control mode. Select any of the following configuration tasks to configure.

- Configuring the MAC-based Control Mode
- Configuring the Port-based Control Mode

1.9.3 Configuring the MAC-based Control Mode

1. Overview

In MAC-based control mode, the MAC address of each client is used as an authentication unit. Clients with different MAC addresses can access network resources only after they pass authentication separately.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the MAC-based control mode.

dot1x port-control-mode mac-based

A port is controlled based on MAC addresses by default.

1.9.4 Configuring the Port-based Control Mode

1. Overview

In port-based control mode, an entire port is used as an authentication unit. As long as one client connected to a port is authenticated, the port is an authenticated port and all clients connected to the port can access network resources.

To allow only one client connected to a port to pass the authentication, you can configure the port-based single-user mode on the basis of port-based control. In this mode, if other users exist on the port, the device deletes all users connected to the port and initiates re-authentication.

2. Restrictions and Guidelines

- In port-based control mode, inter-port migration can be allowed or prohibited for dynamic users. Dynamic users are allowed to migrate between different ports by default.
- In port-based authentication mode, a controlled port supports only one authenticated user while all the users are dynamic users.
- In port-based single-user control mode, only one user on the controlled port can pass authentication and make communication. The limit on the number of users on the port does not affect the limit on the number of users in this mode.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the port-based control mode.

dot1x port-control-mode port-based

A port is controlled based on MAC addresses by default.

(5) (Optional) Configure the port-based single-user control mode.

dot1x port-control-mode port-based single-host

The port-based single-user control mode is not configured by default.

After this command is configured, only one dynamic user can make communication.

(6) (Optional) Disable migration of dynamic users.

dot1x stationarity enable

Migration is allowed for dynamic users by default.

Dynamic users on a controlled port cannot migrate to other ports before aging.

1.10 Configuring Automatic Dynamic VLAN Redirection on IEEE 802.1X Ports

1.10.1 Overview

Automatic dynamic VLAN redirection on IEEE 802.1X ports is used to enable a server to deliver a redirected VLAN. After this function is enabled, when a server delivers a redirected VLAN, relevant users will be added to the redirected VLAN for communication.

The redirection mechanisms implemented by different types of controlled ports are different:

- If controlled ports to be redirected to a VLAN are access ports, trunk ports, or hybrid ports (with MAC VLAN disabled), you can change the native VLANs of these ports to implement dynamic VLAN redirection.
- If controlled ports to be redirected to a VLAN are hybrid ports (with MAC VLAN enabled), you can dynamically create MAC VLAN entries to add authenticated users to the delivered VLAN.

1.10.2 Restrictions and Guidelines

- The device can deliver a VLAN by extending RADIUS attributes. When a RADIUS server delivers a VLAN to an NAS by using an extended attribute, the server encapsulates the extended attribute into RADIUS standard attribute 26. The extended vendor ID is a hexadecimal number 0x00001311. The default type number of the extended attribute is 4. You can run the **radius attribute 4 vendor-type type** command on the device to receive a delivered VLAN whose extended attribute type is **type**.
- The device allows a RADIUS server to deliver VLANs by using RADIUS standard attributes, including a combination of the following attributes:
  - Attribute 64 (**Tunnel-Type**): The value is VLAN (13).
  - Attribute 65 (**Tunnel-Medium-Type**): The value is 802 (6).
  - Attribute 81 (**Tunnel-Private-Group-ID**): The value is a VLAN ID or VLAN name.
- The device can perform IEEE 802.1X authentication on access, trunk, and hybrid ports. If automatic dynamic

VLAN redirection is enabled on other ports, authentication will fail.

- The delivered VLAN attribute is used as a VLAN name. The NAS checks whether a VLAN with the same name is configured. If yes, the NAS automatically adds the user port, to which the VLAN attribute is delivered, to the VLAN. If no VLAN with the same name exists, the delivered VLAN attribute is used as a VLAN ID. If the VLAN ID is valid (within the VLAN ID range supported by the system), the device automatically adds the user port to the VLAN. If the VLAN ID is 0, the device considers no VLAN information delivered. The authentication will fail in other cases.
- Delivered redirected VLANs cannot be private VLANs, remote VLANs, or super VLANs (including sub VLANs).
- When VLAN redirection is configured on an access port and a delivered VLAN does not exist on the device, if the delivered VLAN is identified as a VLAN ID, the device creates the VLAN and adds the port, to which the VLAN attribute is delivered, to the new VLAN, and user authentication succeeds. If the delivered VLAN is identified as a VLAN name, no VLAN ID can be found and user authentication fails. If the delivered VLAN exists on the device and is configured as a redirected VLAN not supported by the access port on the device, users connected to the port will fail the authentication. If the delivered VLAN is configured as a redirected VLAN supported by the access port on the device, the port is removed from its VLAN and added to the delivered VLAN and user authentication succeeds.
- When VLAN redirection is configured on a trunk port and a delivered VLAN does not exist on the device, if the delivered VLAN is identified as a VLAN ID, the device creates the VLAN and changes the native VLAN of the port to the delivered VLAN, and user authentication succeeds. If the delivered VLAN is identified as a VLAN name, no VLAN ID can be found and user authentication fails. If the delivered VLAN exists on the device and is configured as a redirected VLAN not supported by the trunk port (see the description below), the authentication fails. If the delivered VLAN is configured as a redirected VLAN supported by the trunk port on the device, the device changes the native VLAN of the port to the delivered VLAN and user authentication succeeds.
- If the MAC VLAN function is disabled on a hybrid port, a delivered VLAN is processed as follows: If the delivered VLAN does not exist on the device and is identified as a VLAN ID, the device automatically creates the VLAN, allows the VLAN to pass through the current hybrid port in an untagged manner, and changes the native VLAN of the port to the delivered VLAN, and user authentication succeeds. If the delivered VLAN is identified as a VLAN name, no VLAN ID can be found and user authentication fails. If the delivered VLAN exists on the device and is configured as a redirected VLAN not supported by the hybrid port (or the VLAN is contained in the tagged VLAN list of the hybrid port), user authentication fails. Otherwise, the delivered VLAN is allowed to pass through the hybrid port in an untagged manner, the native VLAN of the port is changed to the delivered VLAN, user authentication succeeds.
- If the MAC VLAN function is enabled on a hybrid port, a delivered VLAN is processed as follows: User authentication fails if the VLAN delivered by the authentication server does not exist on the device (the VLAN must be statically configured according to requirements of the MAC VLAN function), the delivered VLAN has been added to the tagged VLAN list of the hybrid port, or the MAC VLAN function does not support the type of the VLAN (for details, see "Configuring MAC VLAN" in the *Ethernet Switching Configuration Guide*). Otherwise, the device dynamically creates MAC VLAN entries based on the delivered VLAN and user MAC addresses, and user authentication succeeds. When a user goes offline, the MAC VLAN entry of the user will be dynamically deleted.
- If the MAC VLAN function is disabled on a port, after a VLAN is delivered, the device changes the native

VLAN of the port but will not change the native VLAN command configuration of the port. The priority of a delivered VLAN is higher than that of a VLAN configured by a command. That is, after successful authentication, the delivered VLAN takes effect, and the native VLAN configured by a command functions after a user goes offline.

- If MAC VLAN is enabled on a port and user authentication is based on MAC addresses, VLANs are delivered through the dynamic creation of MAC VLAN entries, and the native VLAN of the port is not changed.
- No matter whether MAC VLAN is enabled on a hybrid port, if the VLAN delivered via authorization is added to the tagged VLAN list of the port, the VLAN delivery fails.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable automatic dynamic VLAN redirection on the interface.

dot1x dynamic-vlan enable

Dynamic VLAN redirection is disabled on a port by default.

1.11 Configuring the Guest VLAN Function

1.11.1 Overview

The guest VLAN function is used to provide network access permissions for terminals, on which the IEEE 802.1X client is not installed.

After the guest VLAN function is configured, if no IEEE 802.1X client is detected on a controlled port, the port is added to the guest VLAN to allow terminals connected to the port to access network resources in the guest VLAN.

1.11.2 Restrictions and Guidelines

- If a port added to a guest VLAN receives an EAPOL packet, the port is considered to have an IEEE 802.1X-authenticated client attached to it. In this case, the port exits the guest VLAN and performs IEEE 802.1X authentication.
- If any of the following conditions is met, a controlled port is considered to have no IEEE 802.1X-authenticated client attached to it:
  - The port sends an active authentication packet three times consecutively, but receives no EAPOL response packet.
  - The port receives no EAPOL response packet within 90 seconds.
  - The MAC address authentication fails in MAB mode.
- Automatic dynamic VLAN redirection must be enabled on IEEE 802.1X ports.
- When a port switches from Linkup state to Linkdown state, it exits the guest VLAN. When it switches from Linkdown state to Linkup state, the device judges whether the port needs to be added to the guest VLAN.

- After a port fails to receive EAPOL packets within 90s and redirects to a guest VLAN, clients connected to the port need to wait for a long period of time before re-initiating DHCP requests because of the time increment mechanism in the transmission of DHCP discover packets. As a result, it takes a long time for clients to obtain IP addresses after the port redirects to the guest VLAN.
- To configure guest VLAN on a hybrid port, add the VLAN to the untagged VLAN list of the port and then configure the VLAN as a guest VLAN.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the guest VLAN function on the controlled port.

dot1x guest-vlan *vlan-id*

The guest VLAN function is disabled on a controlled port by default.

(Optional) After the guest VLAN function is enabled on a controlled port, the device judges whether the port has an IEEE 802.1X authentication client attached to it. If no, the device adds the port to the guest VLAN.

1.12 Configuring the Failed VLAN Function

1.12.1 Overview

The failed VLAN function is used to provide network access permissions for clients that fail the authentication.

After the failed VLAN function is configured on a port, when the authentication failure count of a client connected to the port reaches the specified number, the port is added to the failed VLAN to allow the client to access network resources in the failed VLAN.

1.12.2 Restrictions and Guidelines

- You can configure the maximum number of consecutive failed authentication attempts for clients. If the authentication failure count of a client reaches this number, the device adds the port connected to the client to a failed VLAN.
- If the failed VLAN configured does not exist, a failed VLAN will be dynamically created when a port is added to the failed VLAN and automatically removed when the port exits the failed VLAN.
- Automatic dynamic VLAN redirection must be enabled on IEEE 802.1X ports.
- When a port switches to Linkdown state, the port automatically exits the failed VLAN.
- The failed VLAN and guest VLAN can be set to the same VLAN.
- In port-based control mode, after a controlled port is added to a failed VLAN, only the users who fail the authentication can re-initiate authentication and other users' authentication requests will be discarded. This restriction does not apply to the MAC-based control mode.
- Private VLANs cannot be configured as 802.1X failed VLANs.

1.12.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure failed VLAN.

dot1x auth-fail vlan *vlan-id*

The failed VLAN function is disabled by default.

(5) (Optional) Configure the maximum number of consecutive failed authentication attempts.

dot1x auth-fail max-attempt *max-attemp-number*

The default maximum number of consecutive failed authentication attempts is **3**.

This command is used to configure the maximum number of times that a user is consecutively rejected by the authentication server. If the rejection count reaches this number, the port, to which the user is connected, will be added to a failed VLAN.

1.13 Configuring Extended Features

1.13.1 Overview

This section describes how to configure some extended features supported by Ruijie devices.

1.13.2 Configuration Tasks

Configure extended features. All the configuration tasks below are optional. Select the configuration tasks as required.

- Enabling Active Authentication
- Configuring a List of Hosts Allowed for Authentication
- Disabling the Virtual Source MAC Address Function
- Configuring Multi-Account Authentication with One MAC Address
- Configuring the Maximum Number of Users Who Can Be Authenticated on an Interface
- Configuring the Function of Initiating Accounting After an IP Address Is Obtained
- Configuring the Priority Order of IEEE 802.1X and MAB
- Configuring the Accounting Update Period
- Configuring Compatibility with H3C Clients and Servers
- Disabling the Global IEEE 802.1X Features

1.13.3 Enabling Active Authentication

1. Overview

Active authentication refers that the NAS actively sends a Request/Identity packet, which triggers IEEE 802.1X clients to initiate IEEE 802.1X authentication.

2. Restrictions and Guidelines

- Some clients use authentication clients embedded in the OS. They may not initiate authentication immediately after connecting to the network, and users cannot use the network promptly. The configured active authentication can urge such clients to initiate authentication in a timely manner after they connect to the network.
- You can use this function to detect whether a client is using Supplicant.
- This function must be configured for MAB deployment.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable active authentication.

dot1x auto-req

The active authentication function is enabled by default.

(4) (Optional) Configure the maximum number of active authentication request packets that can be sent.

dot1x auto-req packet-num *packet-number*

The device always sends authentication request packets actively by default.

(5) (Optional) Configure the interval for sending active authentication request packets.

dot1x auto-req req-interval *req-interval*

The default interval for the device to send active authentication request packets is **30** seconds.

(6) (Optional) Enable the function of detecting whether a user is being authenticated during active authentication.

dot1x auto-req user-detect

The function of detecting whether a user is being authenticated during active authentication is enabled by default.

1.13.4 Configuring a List of Hosts Allowed for Authentication

1. Overview

You can configure only clients with specific MAC addresses connected to specified ports to perform IEEE 802.1X authentication to improve network security.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a list of hosts allowed for authentication.

dot1x auth-address-table address *mac-address* **interface** *interface-type interface-number*

1.13.5 Disabling the Virtual Source MAC Address Function

1. Overview

The virtual source MAC address function enables the device to use a virtual MAC address as the source MAC address of EAP packets in IEEE 802.1X authentication.

This function is used together with Ruijie Supplicant to determine whether an NAS is a Ruijie device. Then, private features can be implemented on Supplicant if the NAS is a Ruijie device. The virtual source MAC address function is enabled by default. You can determine whether to disable the function as required.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable the virtual source MAC address function.

dot1x pseudo source-mac

The source MAC address of IEEE 802.1X packets sent by the device is a virtual MAC address by default.

1.13.6 Configuring Multi-Account Authentication with One MAC Address

1. Overview

The multi-account function allows a user to switch the account upon re-authentication. In some special scenarios in which an account change is needed, such as Windows domain authentication, an access domain is used and an account may be changed for authentication. This function applies to such scenarios.

2. Restrictions and Guidelines

The multi-account authentication function must be disabled if accounting is enabled. Otherwise, accounting may be inaccurate.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable multi-account authentication with one MAC address.

dot1x multi-account enable

Multi-account authentication with one MAC address is disabled by default.

1.13.7 Configuring the Maximum Number of Users Who Can Be Authenticated on an Interface

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of users who can be authenticated on an interface.

dot1x default-user-limit *limit-number*

The maximum number of users who can be authenticated on an interface is unlimited.

1.13.8 Configuring the Function of Initiating Accounting After an IP Address Is Obtained

1. Overview

Clients do not initiate accounting immediately after passing authentication, but wait until they obtain IP addresses.

Some servers request accounting request packets to carry IP addresses. This function can meet this requirement. Authenticated users go online and obtain IP addresses from Supplicant or DHCP snooping. IEEE 802.1X initiates accounting requests only after the users obtain IP addresses. The device may not initiate accounting within a long period of time due to a lack of IP addresses of authenticated clients. For this, the function provides an IP address detection timeout duration. If the device does not obtain the IP address of a client within the timeout duration, the device brings the client offline.

2. Restrictions and Guidelines

- In an IPv4 environment where Ruijie Supplicant client is deployed, Supplicant is capable of uploading IPv4 addresses of clients and therefore, the function does not need to be enabled.
- This function is unavailable in static IP address environments.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of initiating accounting after a user's IP address is obtained.

dot1x valid-ip-acct enable

The function of initiating accounting after a user's IP address is obtained is disabled by default.

(4) Configure the timeout duration for an authenticated user to obtain an IP address.

dot1x valid-ip-acct timeout *timeout*

The default timeout duration for an authenticated user to obtain an IP address is **5** minutes.

1.13.9 Configuring the Priority Order of IEEE 802.1X and MAB

1. Overview

IEEE 802.1X authentication has a higher priority than MAB by default. This function allows you to configure the priority order of IEEE 802.1X authentication and MAB.

If both IEEE 802.1X authentication and MAB are enabled, IEEE 802.1X authentication or MAB is carried out, whichever is triggered first, and IEEE 802.1X authentication is prior to MAB. Therefore, if the device receives an EAPOL packet from a MAB-authenticated user, the device brings the user offline and performs IEEE 802.1X authentication on the user. Currently, the device performs IEEE 802.1X authentication on each user, and then

performs MAB on users who fail the authentication. In addition, MAB takes priority over IEEE 802.1X authentication, and IEEE 802.1X authentication is ignored for MAB-authenticated users.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the priority of IEEE 802.1X authentication to be lower than that of MAB.

dot1x auth-with-order

IEEE 802.1X authentication has a higher priority than MAB by default.

1.13.10 Configuring the Accounting Update Period

1. Overview

Some servers do not deliver the accounting update period during user re-authentication, but require that accounting update packets be sent at the accounting update period delivered at the first authentication. In this case, you can use this function to configure the accounting update period delivered by the server at the first authentication as the accounting update period of re-authentication.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the accounting update period to that delivered by the server at the first authentication.

dot1x acct-update base-on first-time server

The accounting update period delivered by the server at the first authentication is not configured as the accounting update period for re-authentication by default.

1.13.11 Configuring Compatibility with H3C Clients and Servers

1. Overview

This function enables Ruijie devices to be compatible with H3C 802.1X clients and authentication servers.

When 802.1X authentication is performed by a Ruijie device on an H3C iNode, the username provided by the client for authentication uses a special format unrecognized by Ruijie device, resulting in an authentication failure. Usernames required by H3C authentication servers for MAB are in the format of xx-xx-xx-xx-xx-xx, which is different from the default MAB authentication username format of Ruijie devices. As a result, the authentication fails. You can configure this function to implement correct interworking with H3C devices.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the compatibility with H3C 802.1X authentication clients and authentication servers.

dot1x user-name compatible

The compatibility with H3C 802.1X authentication clients and authentication servers is disabled by default.

1.13.12 Disabling the Global IEEE 802.1X Features

1. Overview

You can disable IEEE 802.1X features on all ports at a time.

After global IEEE 802.1X features are disabled, users can access the network without authentication and online users will be brought offline. After global IEEE 802.1X features are enabled, if IEEE 802.1X authentication is configured on a port, users connected to the port need to be authenticated before accessing the network.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable global IEEE 802.1X features.

dot1x system disable

Global IEEE 802.1X features are enabled by default.

1.14 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **dot1x** commands to restore global configuration.

Run the **clear** commands to clear information.

Run the **debug** commands to output debugging information.

Notice

- Running the **clear** commands may lose vital information and thus interrupt services.
- The output debugging information occupies system resources. Therefore, disable the debugging switch immediately after use.

Table 1-1 IEEE 802.1X Monitoring

Command	Purpose
show radius server	Displays the configuration of a RADIUS server.
show dot1x	Displays IEEE 802.1X protocol parameters.

Command	Purpose
show dot1x auth-address-table [**address** *mac-address*] [**interface** *interface-type interface-number*]	Displays the list of hosts allowed for authentication.
show dot1x auto-req	Displays the active authentication status and parameters.
show dot1x port-control [**interface** *interface-type interface-number*]	Displays information about controlled ports.
show dot1x probe-timer	Displays client detection parameters.
show dot1x summary	Displays entries of authenticated users.
show dot1x max-req	Displays the maximum retransmission count of Request/Challenge packets.
show dot1x private-supplicant-only	Displays the status of the non-Ruijie client filtering function.
show dot1x re-authentication	Displays the status of the re-authentication function.
show dot1x reauth-max	Displays the maximum retransmission count of Request/Identity packets.
show dot1x timeout quiet-period	Displays the quiet period after an authentication failure.
show dot1x timeout re-authperiod	Displays the re-authentication interval.
show dot1x timeout server-timeout	Displays the server timeout duration.
show dot1x timeout supp-timeout	Displays the retransmission interval of Request/Challenge packets.
show dot1x timeout tx-period	Displays the retransmission interval of Request/Identity packets.
show dot1x user id *user-id*	Displays details about a user with a specific user ID.
show dot1x user mac *mac-addr*	Displays details about a user with a specific MAC address.
show dot1x user name *user-name*	Displays details about a user with a specific username.
clear dot1x user { **all** | **ip** *ipv4-address* | **mac** *mac-address* | **name** *user-name* }	Deletes an IEEE 802.1X-authenticated user.
dot1x default	Restores the default IEEE 802.1X configuration.
debug aaa	Debugs AAA (for details, see "Configuring AAA").
debug radius	Debugs RADIUS (for details, see "Configuring RADIUS").
debug dot1x event	Debugs IEEE 802.1X events.
debug dot1x packet	Debugs IEEE 802.1X packet processing.

Command	Purpose
debug dot1x stm	Debugs the IEEE 802.1X authentication state machine.
debug dot1x com	Debugs IEEE 802.1X internal communication.
debug dot1x error	Debugs IEEE 802.1X errors.

1.15 Configuration Examples

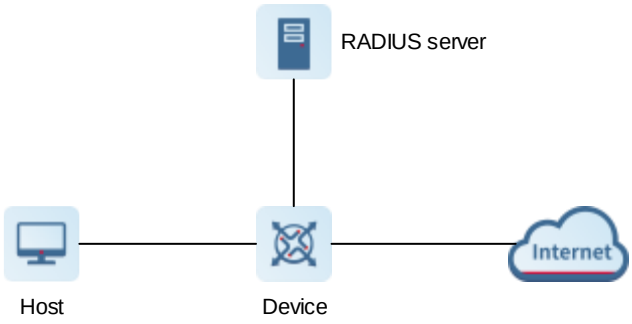
1.15.1 Configuring IEEE 802.1X Authentication

1. Requirements

IEEE 802.1X basic features need to be enabled on a device port so that clients connected to the port can access the network only after passing IEEE 802.1X authentication.

2. Topology

Figure 1-3 Topology of IEEE 802.1X Authentication



3. Notes

- Configure a RADIUS server and add IEEE 802.1X users on the RADIUS server.
- Enable AAA services.
- Configure the server address and key.
- Configure the authentication and accounting method lists.
- Apply the authentication and accounting method lists.
- Enable IEEE 802.1X basic features on an interface.

4. Procedure

(1) Configure a RADIUS server and add an IEEE 802.1X user with the username **hostname1** and password **password1** on the RADIUS server. (The configuration is omitted here. For the configuration of the RADIUS server, see the RADIUS server configuration manual.)

(2) Enable AAA services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

(3) Configure the address and shared key of the AAA server (a RADIUS server is used as an example here, the IP address is set to 192.168.1.3, and the shared key is set to **radiuskey**).

```
Device(config)# radius-server host 192.168.1.3 key radiuskey
```

(4) Configure the authentication and accounting method lists.

```
Device(config)# aaa authentication dot1x auth-method group radius
Device(config)# aaa accounting network account-method start-stop group radius
```

(5) Apply the authentication and accounting method lists.

```
Device(config)# dot1x authentication auth-method
Device(config)# dot1x accounting account-method
```

(6) Enable IEEE 802.1X basic features on an interface.

```
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x port-control auto
```

5. Verification

The user cannot access network resources before authentication, but can access network resources after authentication.

Run the **show dot1x summary** command to display information about the authenticated user.

```
Device# show dot1x summary
ID       Username   MAC           Interface VLAN Auth-State     Backend-State
Port-Status User-Type Time
--------- ---------- --------------  --------- ---- --------------- -------------
----------- --------- ------------------
16778217  hostname1    0023.aeaa.4286  Gi0/1    1   Authenticated   Idle
Authed     static   0days 0h 0m 7s
```

6. Configuration Files

```
!
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
!
```

7. Common Errors

- RADIUS parameters are incorrectly configured.
- A server uses a special access policy, for example, RADIUS packets must carry certain attributes.

- The AAA method list is different from the IEEE 802.1X method list, causing an authentication failure.

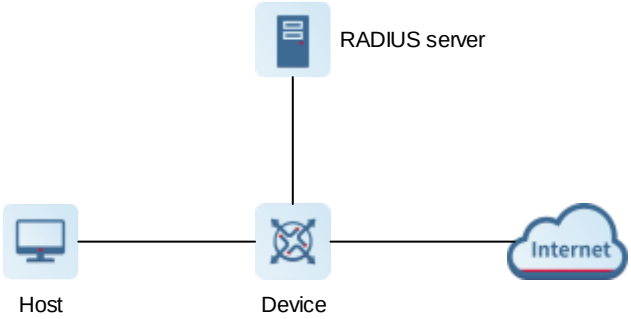
1.15.2 Configuring the IP Authorization Mode

1. Requirements

After IP authorization is configured, only clients with specified IP addresses can pass authentication.

2. Topology

Figure 1-4 Topology of IP Authorization Mode



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Configure the IP authorization mode.

4. Procedure

(1) Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2) Configure the Supplicant authorization mode.

```
Device> enable
Device# configure terminal
Device(config)# aaa authorization ip-auth-mode supplicant
```

5. Verification

A client using a non-specified IP address fails the authentication.

6. Configuration Files

```
!
aaa authorization ip-auth-mode supplicant
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
```

```
!
interface GigabitEthernet 0/1
 dot1x port-control auto
!
```

7. Common Errors

- There are multiple authentication clients in the network. After non-Ruijie client filtering is enabled, some clients fail the authentication.
- Ruijie SAM/SMP is used but SNMP parameters are not configured on the device. As a result, the function of kicking users offline fails.

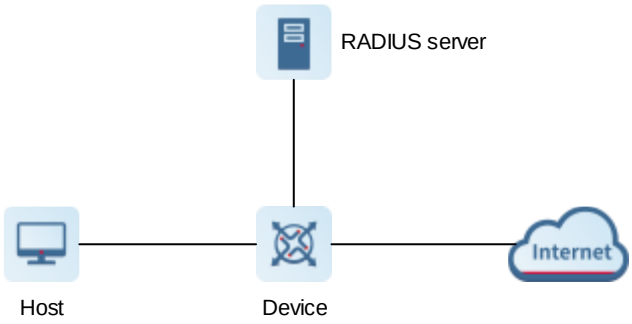
1.15.3 Configuring Multi-user MAB

1. Requirements

Multi-user MAB applies when multiple dumb terminals are connected to one port. After multi-user MAB is configured, each dumb terminal connected to a port needs to be authenticated so that they can access the network.

2. Topology

Figure 1-5 Topology of Multi-user MAB



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Configure multi-user MAB.

4. Procedure

(1) Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2) Configure multi-user MAB.

```
Device> enable
Device# configure terminal
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x mac-auth-bypass multi-user
```

5. Verification

Connect dumb terminals A and B to a port.

(1) If the MAC account of dumb terminal A is added on the RADIUS server, dumb terminal A can access the network properly but dumb terminal B cannot.

(2) Both dumb terminals A and B can access the network properly only after both their MAC accounts are added on the RADIUS server.

6. Configuration Files

```
!
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
 dot1x mac-auth-bypass multi-user
!
```

7. Common Errors

The MAC account format is incorrect on the server.

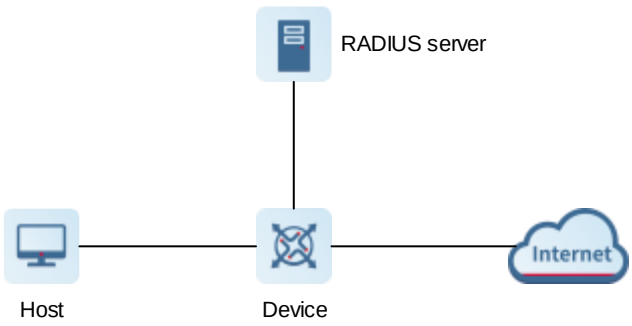
1.15.4 Configuring IAB

1. Requirements

After IAB is configured, when all RADIUS servers configured on the device are unreachable, new access users are allowed to access the network directly.

2. Topology

Figure 1-6 Topology of IAB



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Configure RADIUS server reachability detection.
- Configure IAB.

4. Procedure

(1) Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2) Configure the criteria for judging that a RADIUS server is unreachable as follows: The consecutive timeout count is 5 and the timeout duration is 60 seconds.

```
Device> enable
Device# configure terminal
Device(config)# radius-server dead-criteria time 60 tries 5
```

(3) Configure IAB.

```
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x critical
```

5. Verification

When all RADIUS servers are unreachable, a client can directly access the network after initiating IEEE 802.1X authentication. Authentication will not fail due to the unavailability of RADIUS servers.

6. Configuration Files

```
!
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 test username testname key 7 $10$3b4$ln0s66i8XfEi$
radius-server dead-criteria time 60 tries 5
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
 dot1x critical
!
```

7. Common Errors

- There is a RADIUS server reachable.
- The IEEE 802.1X authentication method list contains other methods besides the RADIUS method.

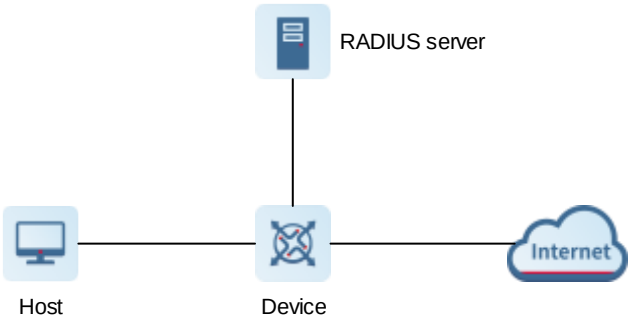
1.15.5 Configuring Automatic Dynamic VLAN Redirection

1. Requirements

After automatic dynamic VLAN redirection is enabled, when the server delivers a redirected VLAN to a port, users connected to the port will be added to the VLAN for communication.

2. Topology

Figure 1-7 Topology of Automatic Dynamic VLAN Redirection



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Enable automatic dynamic VLAN redirection on a controlled port.

4. Procedure

(1) Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2) Enable automatic dynamic VLAN redirection on an interface.

```
Device> enable
Device# configure terminal
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x dynamic-vlan enable
```

5. Verification

Configure the RADIUS server to deliver VLAN attributes. Run the **show dot1x summary** command to display information about the authenticated user. The port, to which the user is connected, redirects from VLAN 2 to VLAN 3.

```
Device# show dot1x summary
ID       Username   MAC           Interface VLAN Auth-State     Backend-State
Port-Status User-Type Time
--------- ---------- --------------  --------- ---- --------------- -------------
----------- --------- ------------------
16778217  Hostname1    0023.aeaa.4286  Gi0/1     3    Authenticated   Idle
Authed      static    0days 2h17m29s
```

6. Configuration Files

```
!
```

```
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
 dot1x dynamic-vlan enable
!
```

7. Common Errors

- RADIUS attributes of the VLAN to be delivered are not correctly configured on the authentication server.
- The RADIUS command for supporting delivered VLAN attributes is not configured on the device.
- When the MAC VLAN configured on a hybrid port is a redirected VLAN, the delivered VLAN is a tagged VLAN.

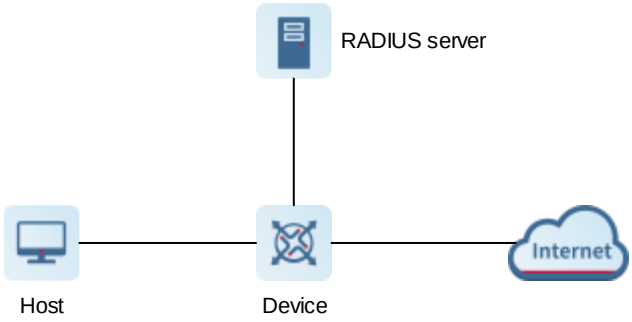
1.15.6 Configuring Guest VLAN

1. Requirements

IEEE 802.1X authentication needs to be enabled on a device port and guest VLAN needs to be configured on the port. If the IEEE 802.1X client is not installed on a terminal connected to the port, the terminal is allowed to access network resources in the guest VLAN.

2. Topology

Figure 1-8 Topology of Guest VLAN



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Enable automatic dynamic VLAN redirection on a controlled port.
- Add the port to a guest VLAN.

4. Procedure

(1) Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2) Enable automatic dynamic VLAN redirection on the port.

```
Device> enable
Device# configure terminal
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x dynamic-vlan enable
```

(3) Add the port to the guest VLAN with the VLAN ID 1.

```
Device(config-if-GigabitEthernet 0/1)# dot1x guest-vlan 1
```

5. Verification

After the port is added to the guest VLAN, the device generates the following log:

```
%DOT1X-5-TRANS_DEFAULT_TO_GUEST: Transformed interface GigabitEthernet 0/1 from
default-vlan 1 to guest-vlan 1 OK.
```

When the IEEE 802.1X client is not configured on a terminal, the terminal can and can only access network resources in VLAN 1 without authentication.

6. Configuration Files

```
!
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
 dot1x dynamic-vlan enable
 dot1x guest-vlan 1
!
```

7. Common Errors

A port receives an EAPOL packet, and as a result, the port cannot be added to a guest VLAN.

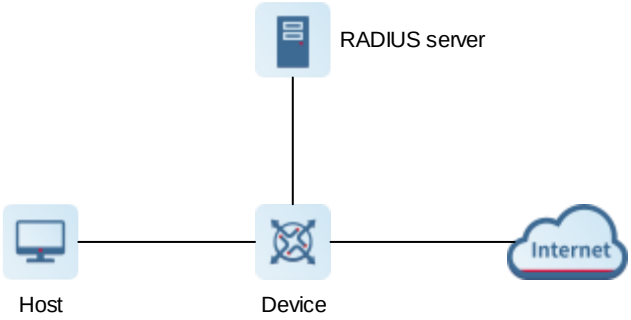
1.15.7 Configuring Failed VLAN

1. Requirements

IEEE 802.1X authentication needs to be enabled on a device port and failed VLAN needs to be configured on the port. If a terminal fails the IEEE 802.1X authentication, it is allowed to access network resources in the failed VLAN.

2. Topology

Figure 1-9 Topology of Failed VLAN



3. Notes

- Enable IEEE 802.1X authentication on a port.
- Add the port to a failed VLAN.

4. Procedure

(1) Enable IEEE 802.1X basic features on a port. For configuration steps, see Configuring IEEE 802.1X Authentication.

(2) Add the port to a failed VLAN with the VLAN ID 1.

```
Device> enable
Device# configure terminal
Device(config)# int gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# dot1x auth-fail vlan 1
```

5. Verification

A terminal cannot access the network before authentication. The terminal uses an incorrect account for authentication. After the authentication fails, the terminal can access network resources in the failed VLAN.

6. Configuration Files

```
!
dot1x authentication auth-method
dot1x accounting account-method
!
aaa new-model
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
aaa accounting network account-method start-stop group radius
aaa authentication dot1x auth-method group radius
!
interface GigabitEthernet 0/1
 dot1x port-control auto
```

```
 dot1x auth-fail vlan 1
!
```

7. Common Errors

If a user fails the authentication not due to the rejection from the authentication server, for example, the authentication client cannot be installed because of underlying resource insufficiency, the user will not be added to a failed VLAN.

Contents

1 Configuring Web Authentication 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 8
1.2 Restrictions and Guidelines 9
1.3 Configuration Task Summary 9
1.4 Configuring Ruijie First-Generation Web Authentication 10
1.4.1 Overview 10
1.4.2 Restrictions and Guidelines 10
1.4.3 Prerequisites 11
1.4.4 Procedure 11
1.5 Configuring Ruijie Second-Generation Web Authentication 12
1.5.1 Overview 12
1.5.2 Restrictions and Guidelines 13
1.5.3 Prerequisites 13
1.5.4 Procedure 13
1.6 Configuring App-based Authentication 15
1.6.1 Overview 15
1.6.2 Restrictions and Guidelines 15
1.6.3 Procedure 15
1.7 Configuring an Authentication Method List 16
1.7.1 Overview 16

1.7.2 Restrictions and Guidelines 16

1.7.3 Procedure 16

1.8 Configuring an Accounting Method List 17

1.8.1 Overview 17

1.8.2 Restrictions and Guidelines 17

1.8.3 Procedure 17

1.9 Configuring the Portal Communication Destination Port 17

1.9.1 Overview 17

1.9.2 Restrictions and Guidelines 17

1.9.3 Procedure 17

1.10 Configuring the Binding Mode 18

1.10.1 Overview 18

1.10.2 Restrictions and Guidelines 18

1.10.3 Procedure 18

1.11 Configuring the Redirection HTTP Port 19

1.11.1 Overview 19

1.11.2 Restrictions and Guidelines 19

1.11.3 Procedure 19

1.12 Configuring the Redirection Connection Timeout Time 19

1.12.1 Overview 19

1.12.2 Procedure 19

1.13 Configuring Portal Detection 20

1.13.1 Overview 20

1.13.2 Restrictions and Guidelines 20

1.13.3 Procedure....20

1.14 Configuring Portal Escape....20

1.14.1 Overview....20

1.14.2 Restrictions and Guidelines....21

1.14.3 Procedure....21

1.15 Configuring the Portal Communication Source Port....21

1.15.1 Overview....21

1.15.2 Restrictions and Guidelines....21

1.15.3 Procedure....21

1.16 Disabling Portal Specification Extension....21

1.16.1 Overview....21

1.16.2 Restrictions and Guidelines....22

1.16.3 Procedure....22

1.17 Configuring Transparent Transmission of RADIUS Private Attributes....22

1.17.1 Overview....22

1.17.2 Restrictions and Guidelines....22

1.17.3 Procedure....22

1.18 Configuring the Authentication-Free Network Resource Range....23

1.18.1 Overview....23

1.18.2 Restrictions and Guidelines....23

1.18.3 Procedure....23

1.19 Configuring a Straight-through ARP Resource Range....23

1.19.1 Overview....23

1.19.2 Restrictions and Guidelines....23

1.19.3 Procedure....24

1.20 Configuring an Authentication-Exempted User Range....24

1.20.1 Overview....24

1.20.2 Restrictions and Guidelines....24

1.20.3 Procedure....24

1.21 Configuring Logging of the Web Authentication Module....25

1.21.1 Overview....25

1.21.2 Restrictions and Guidelines....25

1.21.3 Procedure....25

1.22 Configuring the Maximum Number of HTTP Sessions for Unauthenticated Users....25

1.22.1 Overview....25

1.22.2 Restrictions and Guidelines....25

1.22.3 Procedure....25

1.23 Configuring the Interval for Updating Online User Information....26

1.23.1 Overview....26

1.23.2 Restrictions and Guidelines....26

1.23.3 Procedure....26

1.24 Enabling DHCP Address Check....26

1.24.1 Overview....26

1.24.2 Restrictions and Guidelines....26

1.24.3 Procedure....27

1.25 Configuring an Address Whitelist....27

1.25.1 Overview....27

1.25.2 Restrictions and Guidelines....27

1.25.3 Procedure....27

1.26 Configuring VLAN-based Authentication on a Port....28

1.26.1 Overview....28

1.26.2 Restrictions and Guidelines....28

1.26.3 Procedure....28

1.27 Configuring the Authenticated User Logout Delay on a Port....28

1.27.1 Overview....28

1.27.2 Restrictions and Guidelines....28

1.27.3 Procedure....28

1.28 Enabling RADIUS Server Escape....29

1.28.1 Overview....29

1.28.2 Restrictions and Guidelines....29

1.28.3 Procedure....29

1.29 Configuring DHCP Server Detection....29

1.29.1 Overview....29

1.29.2 Restrictions and Guidelines....29

1.29.3 Procedure....29

1.30 Configuring Uniqueness Check of Portal Authentication Accounts....30

1.30.1 Overview....30

1.30.2 Procedure....30

1.31 Enabling Automatic Adding of Domain Information After Usernames....30

1.31.1 Overview....30

1.31.2 Restrictions and Guidelines....30

1.31.3 Procedure....30

1.32 Configuring HTTPS Certificate Import 31

1.32.1 Overview 31

1.32.2 Procedure 31

1.33 Enabling Adding the Authentication Page to Favorite 31

1.33.1 Overview 31

1.33.2 Restrictions and Guidelines 31

1.33.3 Procedure 31

1.34 Configuring a Template Mapping Method 32

1.34.1 Overview 32

1.34.2 Restrictions and Guidelines 32

1.34.3 Procedure 32

1.35 Monitoring 32

1.36 Configuration Examples 34

1.36.1 Configuring First-Generation Web Authentication 34

1.36.2 Configuring Second-Generation Web Authentication 36

1 Configuring Web Authentication

1.1 Introduction

1.1.1 Overview

Web authentication is an identity authentication method for controlling users' network access permissions. When an unauthenticated user attempts to access the Internet through a browser, the network access server (NAS) forcibly redirects the browser to a specified site (portal server). The user can access services of the portal server without authentication. If the user wants to access network resources beyond the portal server, the user must pass through authentication.

Web authentication has the following advantages:

- Convenient to use: Users do not need to install dedicated client software and can complete authentication through a browser.
- Personalized services and service extension: Through interaction between the browser and the portal server, users can customize services, such as advertisements, notifications, and business links on the portal server page.

1.1.2 Principles

1. Basic Concepts

- Authentication client

  Generally, an authentication client refers to a browser running Hypertext Transfer Protocol (HTTP). When a user accesses the Internet via a browser, the browser will send HTTP requests.

- NAS

  Generally, the NAS refers to an access-layer device in a network. It is directly connected to user hosts and needs to be enabled with web authentication.

- Portal server

  The portal server provides the web authentication page to interact with user hosts.

- RADIUS server

  The RADIUS server provides RADIUS-based remote user authentication.

- HTTP interception

  HTTP interception means that the NAS intercepts to-be-forwarded HTTP packets.

  These HTTP packets are sent by the browsers of the user hosts connected to the NAS but they are not destined for the NAS. For example, a user accesses www.google.com via the Internet Explorer (IE). The NAS is supposed to forward the HTTP request packets from the user to the gateway. If HTTP interception is enabled, these packets will not be forwarded.

  HTTP interception is the foundation of web authentication. Web authentication is triggered automatically once HTTP interception succeeds.

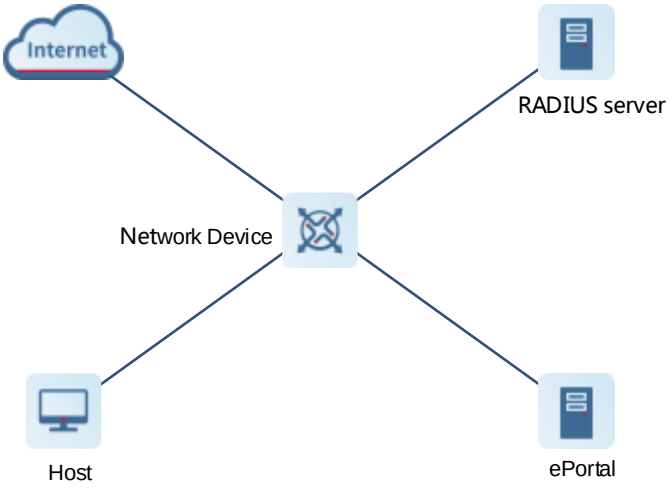
- HTTP redirection

In normal cases, after a user host sends an HTTP GET or HEAD request through a browser, the receiver responds with a 200 response if it can provide resources and a 302 response if it cannot provide resources. The 302 response provides a new site path. After receiving the response, the user host can send an HTTP GET or HEAD packet to the new site to request resources. This is called redirection.

2. Web Authentication Solutions

Ruijie web authentication has multiple versions that use different web authentication processes. Currently, Ruijie first-generation and second-generation web authentications are supported. You can select a version based on your actual requirements.

Figure 1-1 Typical Networking for Web Authentication



- Ruijie first-generation web authentication

  Ruijie first-generation web authentication requires cooperation of the Ruijie dedicated ePortal server. The ePortal server provides the authentication and accounting functions, which relieves the NAS from service burden.

  The authentication process is as follows:
  A user submits authentication information through the authentication page provided by the ePortal server.
  The ePortal server initiates an authentication request to the RADIUS server.
  After authentication succeeds, the ePortal server sends the user information to the NAS through Simple Network Management Protocol (SNMP).
  The NAS controls user access permissions.

- Ruijie second-generation web authentication

  Ruijie second-generation web authentication complies with the China Mobile Communications Corporation (CMCC) WLAN Service Portal Specification that is widely used in the industry. The portal server is responsible for interaction on the user page only and is easily compatible with products of different vendors. However, the main authentication process is performed on the NAS, and therefore higher requirements are raised for the NAS.

  The authentication process is as follows:
  A user submits authentication information through the authentication page provided by the portal server.
  The portal server informs user identity information to the NAS through the portal protocol. The NAS initiates

an authentication request to the RADIUS server using the identity information, assigns access permissions to authenticated users, and returns authentication results to the portal server.

- Web authentication solutions

Table 1-1 Web Authentication Solutions

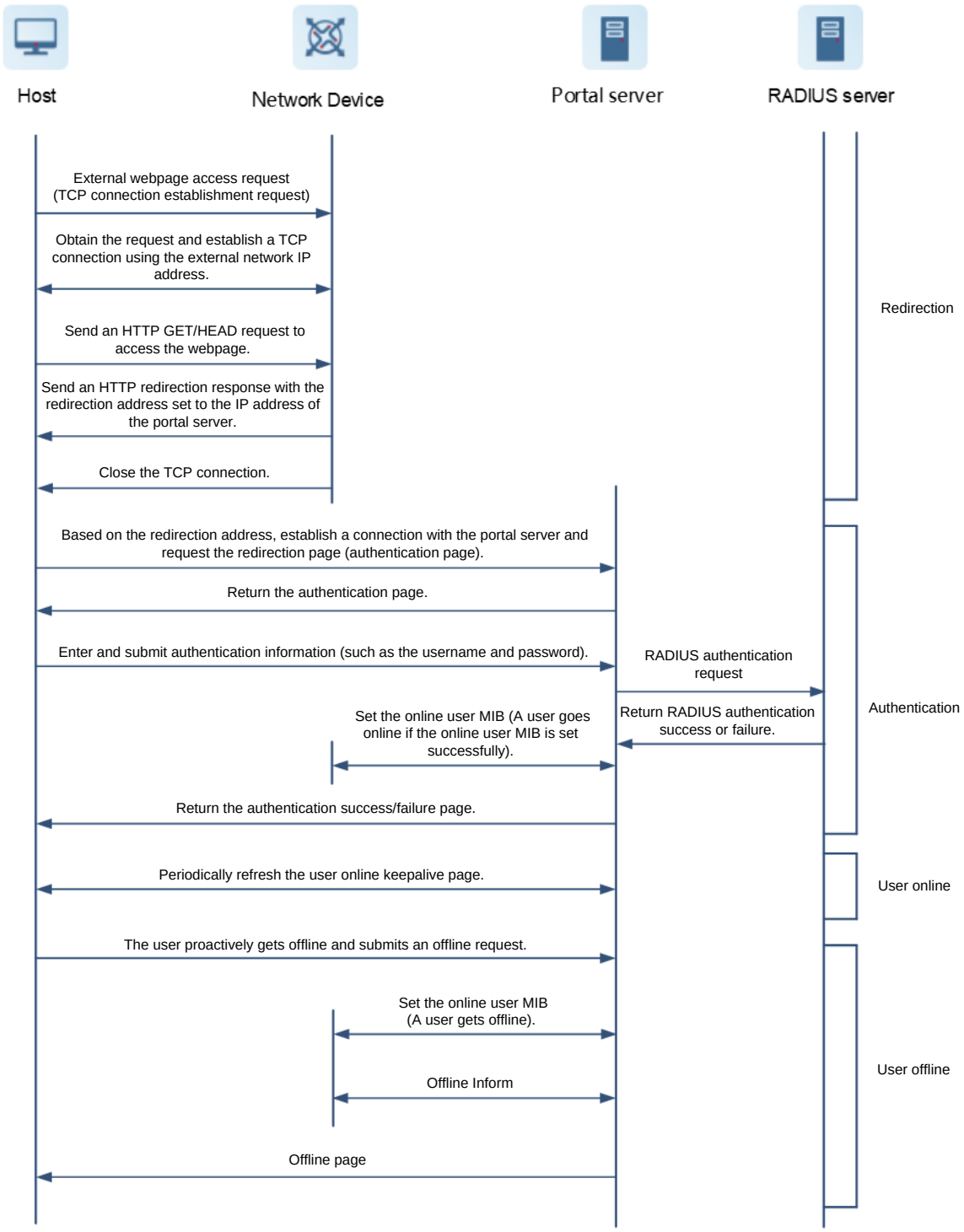
		Ruijie First-Generation Web Authentication	Ruijie Second-Generation Web Authentication
Authentication roles	Client	In these two authentication solutions, clients have the same functions.	
	NAS	The NAS redirects users and exchanges user online/offline notifications with the portal server.	The NAS redirects and authenticates users, and notifies the portal server of the authentication results.
	Portal server	The portal server interacts with clients through the authentication page, authenticates users, and notifies the NAS of the authentication results.	The portal server interacts with clients through the authentication page, notifies the NAS of users' authentication information, and receives the authentication results from the NAS.
	RADIUS server	In these two authentication solutions, the RADIUS servers have the same functions.	
Authentication process	Authentication and accounting	The portal server initiates authentication and accounting to the RADIUS server.	The NAS initiates authentication and accounting to the RADIUS server.
Offline process	Offline action	An offline action may be triggered by a notification from the portal server and traffic detection or port status detection performed by the NAS.	An offline action may be triggered by a notification from the portal server, a kickout notification from the RADIUS server, and traffic detection or port status detection performed by the NAS.
	Accounting completion packet	Accounting completion packets are initiated by the portal server.	Accounting completion packets are initiated by the NAS.

Instruction

- The web authentication solution is selected based on the type of the portal server in use.
- Some parameters can be shared by different web authentication solutions but some are not. Distinguish these parameters carefully to avoid abnormal web authentication due to parameter misconfiguration.

3. Ruijie First-Generation Web Authentication

Figure 1-2 Flowchart of Ruijie First-Generation Web Authentication



As shown in Figure 1-2, the Ruijie first-generation web authentication process includes four phases: redirection, authentication, user online, and user offline.

(1) Redirection

Before authentication, the NAS intercepts all HTTP requests from unauthenticated users and redirects these requests to the portal server. An authentication page is displayed on the browser of a user.

(2) Authentication

During authentication, the user enters information, for example, the username, password, and verification code on the web authentication page to interact with the portal server and complete authentication.

(3) User online

After the user succeeds in the authentication, the portal server notifies the NAS that the user has been authenticated. The NAS allows the user to access Internet resources.

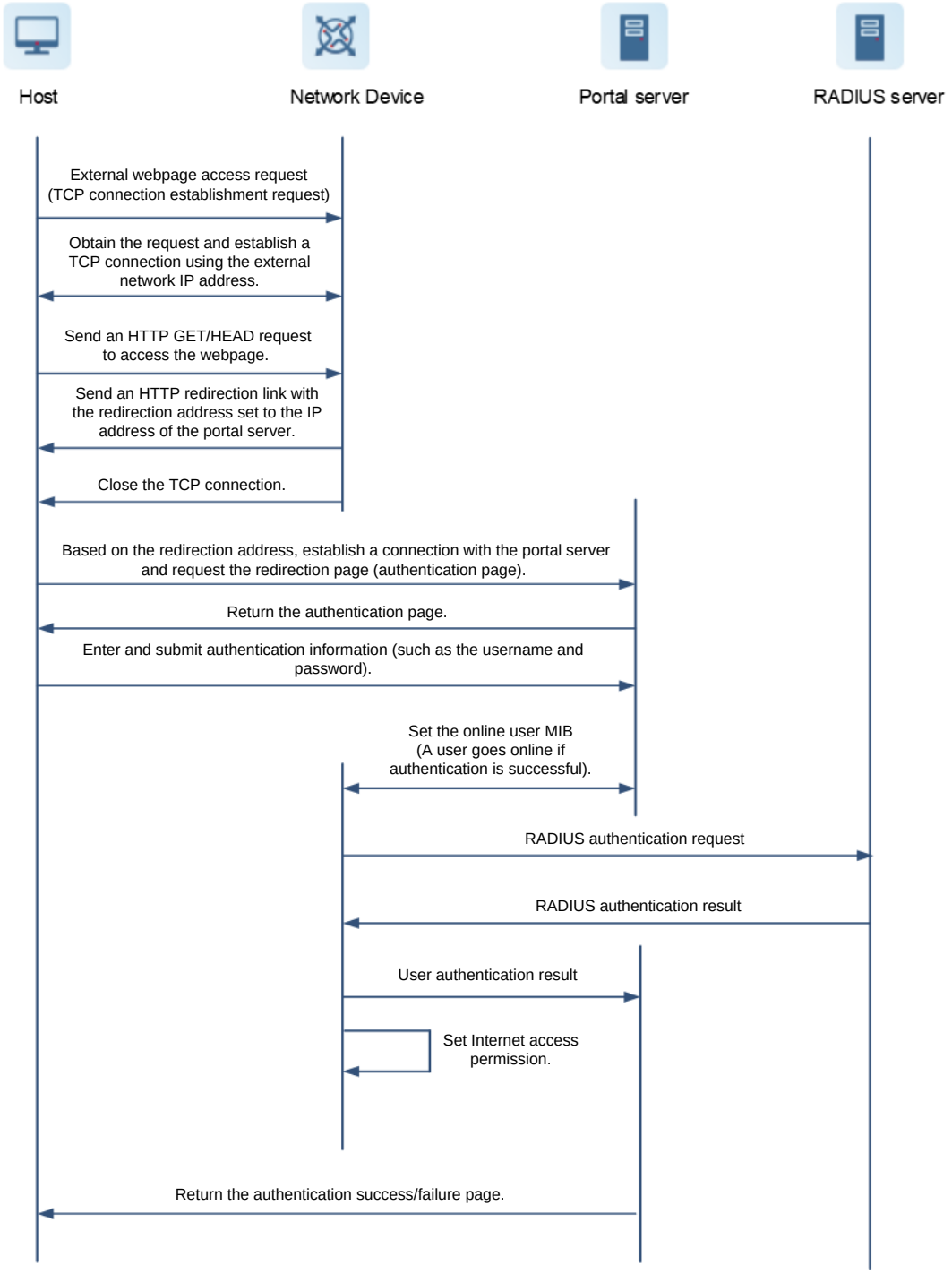
(4) User offline

After the user gets offline, the portal server sends an accounting completion request to the RADIUS server and notifies the RADIUS server that the user has gotten offline. There are two user offline detection types:

- The NAS detects offline of a user when the user's time is due, the data quota is reached, or the link is disconnected. The NAS will notify the portal server of a user offline message. After receiving the message, the portal server requires the NAS to delete user information through SNMP and returns the offline page to the user host.
- The portal server detects getting offline of a user when the user triggers an offline request through the offline page or the keepalive page becomes invalid. The portal server notifies the NAS of a user offline message and returns the offline page to the user host.

4. Ruijie Second-Generation Web Authentication

Figure 1-3 Flowchart of Ruijie Second-Generation Web Authentication



- Authentication process

  a Before authentication, the NAS intercepts all HTTP requests from unauthenticated users and redirects these requests to the portal server. An authentication page is displayed on the browser of a user.

  b The user enters authentication information, such as the username, password, and verification code on the authentication page to interact with the portal server.

  c The portal server sends the user authentication information to the NAS.

d The NAS initiates authentication to the RADIUS server and returns the authentication result to the portal server.

e The portal server displays the authentication result (success or failure) to the user on a page.

- User offline

  There are two user offline detection types: (1) The NAS detects offline of a user when the user's time is due, the data quota is reached, or the link is disconnected. (2) The portal server detects offline of a user when the user triggers an offline request through the offline page.

  Common offline scenarios are as follows:

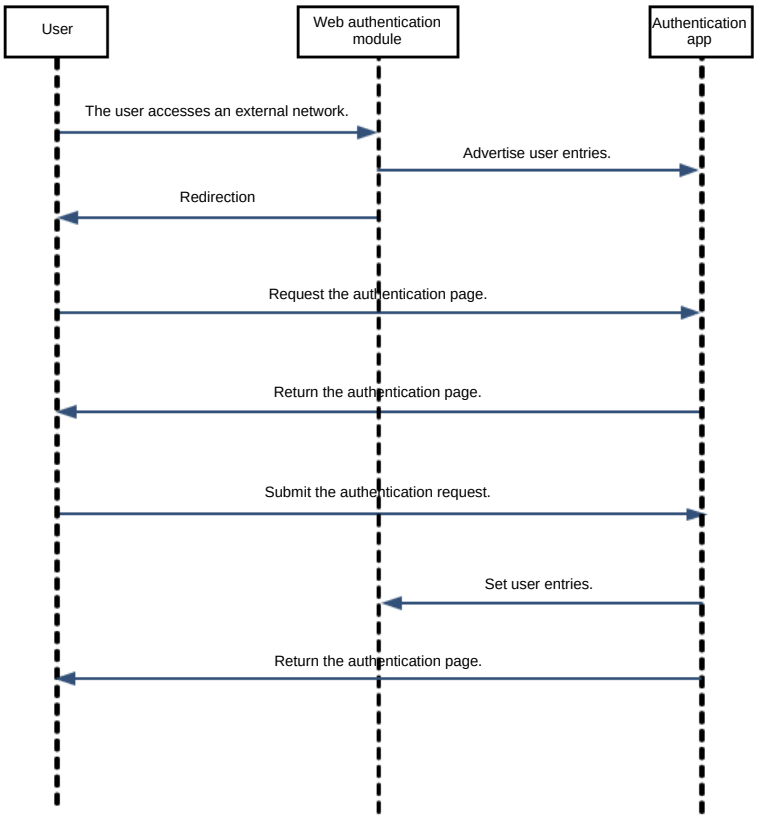
  - When a user clicks the Logout button on the page, the portal server instructs the NAS to get the user offline.
  - The NAS forces a user offline when detecting that the traffic of the user is lower than the threshold, depending on the configured traffic threshold detection parameter.
  - When the RADIUS server plans to force a user offline based on a certain policy, the NAS instructs the portal server to push an offline page to the user host.

5. App-based Authentication

App-based authentication is actually performed by a third-party app. The web authentication module is not responsible for authentication. It serves as an agent to connect the user host and authentication app.

- Main roles
  - User host: user host to be authenticated when accessing network resources.
  - Webauth: web authentication component that is responsible only for redirection and user entry settings and not for interaction with the server.
  - Authentication app: performs authentication.
- Authentication process

Figure 1-4 Flowchart of App-based Web Authentication



As shown in Figure 1-4, the authentication app interacts with the server, and the web authentication component does not need to care about the internal authentication process of the authentication app. In the preceding figure, the portal server role is not provided. The app-based authentication process is as follows:

a A user host accesses an external network and triggers HTTP redirection. Webauth creates a user and advertises it to the authentication app.

b The user host accesses the redirection page.

c The user submits an authentication request on the login page.

d The authentication app authenticates the user. After authentication succeeds, the authentication app sends a message to Webauth to allow packets from the user to pass through.

e The authentication app returns the authentication result to the user host.

1.1.3 Protocols and Standards

- RFC1945: Hypertext Transfer Protocol -- HTTP/1.0
- RFC2068: Hypertext Transfer Protocol -- HTTP/1.1
- RFC2818: HTTP Over TLS
- RFC1157: Simple Network Management Protocol (SNMP)
- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

1.2 Restrictions and Guidelines

- Different web authentication versions are highly divergent in the authentication processes and configurations. Read the relevant chapters carefully before configuring functions related to web authentication to prevent misconfiguration.
- Ruijie second-generation web authentication supports local account authentication on the NAS. Because RADIUS authentication is more commonly used in networks, it is generally used in application examples.
- Web authentication supports the authentication of domain names. That is, accounts can be authenticated in the format of user name@domain name. This requires enabling the domain-name-based authentication, authorization and accounting (AAA) service. For details, see "Configuring AAA" in the *Security Configuration Guide*.

1.3 Configuration Task Summary

Web authentication configuration includes the following tasks:

(1) Configure basic web authentication functions. Select any of the following configuration tasks to configure.

- Configuring Ruijie First-Generation Web Authentication
- Configuring Ruijie Second-Generation Web Authentication
- Configuring App-based Authentication

(2) (Optional) Configure web authentication template attributes. Perform the following optional configuration tasks as required.

- Configuring an Authentication Method List
- Configuring an Accounting Method List
- Configuring the Portal Communication Destination Port
- Configuring the Binding Mode

(3) (Optional) Configure parameters for communicating with the portal server. Perform the following optional configuration tasks as required.

- Configuring the Redirection HTTP Port
- Configuring the Redirection Connection Timeout Time
- Configuring Portal Detection
- Configuring Portal Escape
- Configuring the Portal Communication Source Port
- Disabling Portal Specification Extension

(4) (Optional) Configure authentication-free resources. Perform the following optional configuration tasks as required.

- Configuring the Authentication-Free Network Resource Range
- Configuring a Straight-through ARP Resource Range
- Configuring an Authentication-Exempted User Range

(5) (Optional) Configure user management functions. Perform the following optional configuration tasks as required.

- Configuring Logging of the Web Authentication Module
- Configuring the Maximum Number of HTTP Sessions for Unauthenticated Users
- Configuring the Interval for Updating Online User Information
- Enabling DHCP Address Check
- Configuring an Address Whitelist
- Configuring VLAN-based Authentication on a Port
- Configuring the Authenticated User Logout Delay on a Port
- Enabling RADIUS Server Escape
- Configuring DHCP Server Detection
- Configuring Uniqueness Check of Portal Authentication Accounts
- Enabling Automatic Adding of Domain Information After Usernames

(6) (Optional) Configure other functions. Perform the following optional configuration tasks as required.

- Configuring Transparent Transmission of RADIUS Private Attributes
- Configuring HTTPS Certificate Import
- Enabling Adding the Authentication Page to Favorite
- Configuring a Template Mapping Method

1.4 Configuring Ruijie First-Generation Web Authentication

1.4.1 Overview

After Ruijie first-generation web authentication is enabled, unauthenticated users will be redirected to the authentication page for authentication.

When an unauthenticated user attempts to access network resources, the NAS redirects the user to the authentication page, where the user can initiate authentication to the portal server.

1.4.2 Restrictions and Guidelines

- To apply web authentication successfully, you need to configure and apply a portal server.
- To apply web authentication successfully, you need to configure the key used for the communication between the access or convergence device and the portal server.
- To apply web authentication successfully, you need to configure the SNMP parameters used for the communication between the NAS and portal server. For more information about SNMP, see "Configuring SNMP" in the *Network Management and Monitoring Configuration Guide*.
- When the access or convergence device finds an unauthenticated user attempting to access network resources through HTTP, it redirects the access request to the specified portal authentication page, where the user can initiate authentication to the portal server. Unauthenticated users can directly visit the IP address of the portal server only if the IP address is configured as an authentication-free network resource.
- When web authentication is enabled in interface configuration mode, it is disabled by default. Web authentication is not performed on user hosts connected to the port.

1.4.3 Prerequisites

Valid to-be-authenticated user information is configured on the RADIUS server. For details about configuration of to-be-authenticated user information, see the user manual of the RADIUS server.

1.4.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Create a first-generation web authentication template and enter the template configuration mode.

web-auth template eportalv1

(5) Configure parameters for interaction between the NAS and portal server.

a Configure the IP address and virtual routing and forwarding (VRF) instance of the portal server.

ip [*ip-address* | **oob** | **vrf** *vrf-name*]

No portal server IP address or VRF instance is configured by default.

After this command is configured, the NAS allows server access requests and can set a rate limit for requests sent to the server.

b Configure the authentication page address of the portal server.

url *url-string*

No authentication page address of the portal server is configured by default.

The URL to which a user is redirected is usually the authentication page address of the portal server.

c Configure the URL format of redirection packets.

fmt { **ace** | **default** }

The Ruijie URL format is used for redirection packets by default.

Access control entry (ACE) association is supported when **fmt** is set to **ace**.

d Configure the binding mode used by a template.

bindmode { **ip**-**mac**-**mode** | **ip**-**only**-**mode** }

The default binding mode used by a template is IP address+MAC address.

e Configure the encapsulation format of redirection packets.

redirect { **http** | **js** }

Redirection packets of the Ruijie URL format use the JavaScript (JS) encapsulation format, and redirection packets of CMCC-related URL formats use the HTTP encapsulation format by default.

Some apps cannot execute JS actions, and packets need to be encapsulated in HTTP format to trigger redirection.

(6) Return to the global configuration mode.

exit

(7) Configure the communication key between the NAS and the portal server.

web-auth portal key *key*

No communication key between the NAS and the portal server is configured by default.

During authentication, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

(8) Configure SNMP parameters.

The NAS and portal server use SNMP to manage users to be authenticated. SNMPv2 and SNMPv3 are available.

SNMPv2 is used as an example here. If high security requirements are raised, you are advised to use SNMPv3.

a Configure the SNMP community string on the NAS for the portal server to manage online users on the NAS.

snmp-server community { *community-string* } **rw**

The portal server uses the SNMP community string to read/write user information from/to the NAS.

b Configure the SNMP server.

snmp-server host { *ip-address* } **inform version 2c** { *community-string* } **web-auth**

The NAS sends Inform/Trap packets to notify the portal server of user offline.

c Enable the Webauth Trap/Inform function.

snmp-server enable traps web-auth

The Webauth Trap/Inform function is configured to enable the NAS to inform the portal server of user offline.

(9) Enter the interface configuration mode.

interface *interface-type interface-number*

(10) Enable first-generation web authentication on a port.

web-auth enable

The web authentication function is disabled on a port by default.

1.5 Configuring Ruijie Second-Generation Web Authentication

1.5.1 Overview

After Ruijie second-generation web authentication is enabled, unauthenticated users will be redirected to the authentication page for authentication.

When an unauthenticated user attempts to access network resources, the NAS redirects the user to the authentication page, where the user can initiate authentication to the portal server.

1.5.2 Restrictions and Guidelines

Ruijie second-generation web authentication complies with the *CMCC WLAN Service Portal Specification*. Furthermore, it is extended to support the Ruijie ePortal server. In actual deployment, compatible configuration is required based on the server performance.

1.5.3 Prerequisites

Authenticated user information is configured on the RADIUS server. For details about user information configuration on the RADIUS server, see the configuration guide of the RADIUS server.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

In Ruijie second-generation web authentication, the NAS initiates authentication to the portal server through the AAA module.

(4) Configure the address, port number, and key of the RADIUS server.

radius-server host { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port-number*] [**acct-port** *acct-port-number*] [**key** [**0** | **7**] *text-string*]

No RADIUS server IP address, port number, or key is configured by default. The default authentication port is **1812** and the default accounting port is **1813**.

Users' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a user.

(5) Configure a second-generation web authentication method list.

aaa authentication web-auth { **default** | *list-name* } { [**group** *group-name*]&<1-4> | **group radius** | **local** | **none** } *

No second-generation web authentication method list is configured by default.

A web authentication method list associates web authentication requests with the RADIUS server. The NAS selects an authentication method and a server based on the web authentication method list.

(6) Configure a network accounting method list.

aaa accounting network { **default** | *list-name* } **start-stop** { [**group** *group-name*]&<1-4> | **group radius** | **group tacacs+** | **none** } *

The web accounting function is disabled by default.

An accounting method list associates an accounting method and server. In web authentication, accounting is implemented to record user information or fees.

(7) Create a second-generation web authentication template and enter the template configuration mode.

web-auth template eportalv2

(8) Configure web authentication template parameters.

a Configure an authentication method list for the template.

authentication *method-list*

The default authentication method list is used by a template by default.

b Configure the accounting method list used by a template.

accounting *method-list*

The default accounting method list is used by a template by default.

c Configure the IP address and VRF instance of the portal server.

ip [*ip-address* | **oob** | **vrf** *vrf-name*]

No portal server IP address or VRF instance is configured by default.

d Configure the authentication page address of the portal server.

url *url-string*

The authentication page address of the portal server is configured by default.

When you configure the URL of the second-generation portal server, if the URL contains an IPv6 address, enclose it with a pair of square brackets. For example, when the IPv6 address is 2001::1, the actual configured URL is http://[2001::1]/index.jsp. The IPv6 template does not support **fmt** configuration.

e Configure the URL format of redirection packets.

fmt { **cmcc-ext1** | **cmcc-ext2** | **cmcc-ext3** | **cmcc-mtx** | **cmcc-normal** | **ct-jc** | **cucc** | **default** }

The Ruijie URL format is used for redirection packets by default.

When **fmt** is set to **cmcc-normal** or **cmcc-ext1**, only the IPv4 format is supported.

f Configure the binding mode used by a template.

bindmode { **ip-mac-mode** | **ip-only-mode** }

The default binding mode used by a template is IP address+MAC address.

g Configure the encapsulation format of redirection packets.

redirect { **http** | **js** }

Redirection packets of the Ruijie URL format use the JS encapsulation format, and redirection packets of the CMCC-related URL formats use the HTTP encapsulation format by default.

(9) Return to the global configuration mode.

exit

(10) Configure the communication key between the NAS and the portal server.

web-auth portal key *key*

No communication key between the NAS and the portal server is configured by default.

(11) Enter the interface configuration mode.

interface *interface-type interface-number*

(12) Enable second-generation web authentication on a port.

web-auth enable eportalv2

1.6 Configuring App-based Authentication

1.6.1 Overview

The authentication app can interwork with the web authentication component to redirect unauthenticated users to the authentication page for authentication.

1.6.2 Restrictions and Guidelines

In template configuration mode, the authentication app name must be correctly configured.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an app-based authentication template and enter the template configuration mode.

web-auth template appauth

(4) Configure the authentication app name in the template.

app-name { **APP_AUTH** | *app-name* }

(5) Configure attribute parameters of the app-based authentication template.

a Configure the IP address and VRF instance of the portal server.

ip [*ip-address* | **oob** | **vrf** *vrf-name*]

No portal server IP address or VRF instance is configured by default.

b Configure the communication port of the portal server.

port *port-number*

The default communication port of the portal server is **80**.

c Configure the authentication page address of the portal server.

url *url-string*

The authentication page address of the portal server is configured by default, and must be started with http:// or https://.

d Configure the binding mode used by a template.

bindmode { **ip-mac-mode** | **ip-only-mode** }

The default binding mode used by a template is IP address+MAC address.

e Configure the encapsulation format of redirection packets.

redirect { **http** | **js** }

Redirection packets of the Ruijie URL format use the JS encapsulation format, and redirection packets of the CMCC-related URL formats use the HTTP encapsulation format by default.

When some apps cannot execute JS actions, packets need to be encapsulated in HTTP format to trigger redirection.

f Configure the IP address of the NAS.

nas-ip { *ipv4-address* }

No NAS IP address is configured by default.

During app-based authentication, **nas-ip** is used only to specify the redirection URL transmitted to the portal server. If **nas-ip** is not configured, the local device address is automatically obtained based on the server IP address as **nas-ip**.

(6) Return to the global configuration mode.

exit

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Enable app-based authentication on a port.

web-auth enable appauth

1.7 Configuring an Authentication Method List

1.7.1 Overview

After an authentication method list is configured, the NAS selects a server for authentication based on the specified authentication method list.

When a user submits authentication information, the portal server sends an authentication request to the NAS. The NAS resolves the authentication server and other information based on the configured authentication method list name before initiating authentication.

1.7.2 Restrictions and Guidelines

- Before you configure an authentication method list, ensure that the authentication methods in the list have been configured on the AAA module.
- The same authentication method needs to be used for IPv4 and IPv6 packets.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the web authentication template configuration mode.

web-auth template { **eportalv2** | *template-name* **v2** }

(4) Configure an authentication method list for the template.

authentication *method-list*

The default authentication method list is used by a template by default.

1.8 Configuring an Accounting Method List

1.8.1 Overview

After an accounting method list is configured, the NAS selects a server for accounting based on the specified accounting method list.

After a user passes authentication, the NAS sends an accounting request. The recipient of the request depends on the configuration of the accounting method list and is usually the portal server.

1.8.2 Restrictions and Guidelines

- Before you configure an accounting method list, ensure that the accounting methods in the list have been configured on the AAA module.
- The same accounting method needs to be used for IPv4 and IPv6 packets.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the web authentication template configuration mode.

web-auth template { **eportalv2** | *template-name* **v2** }

(4) Configure the accounting method used by a template.

accounting *method-list*

The default accounting method list is used by a template by default.

1.9 Configuring the Portal Communication Destination Port

1.9.1 Overview

After the portal communication destination port is configured, the NAS regards the port as the communication port of the portal server, monitors packets from the portal server over this port, and specifies this port in packets sent to the portal server.

The NAS interacts with the portal server through the portal protocol, which specifies the port number used to listen to and send/receive packets. When the NAS detects that a user gets offline, it notifies the portal server. When the portal server listening port is changed, the NAS needs to re-configure the portal server communication port.

1.9.2 Restrictions and Guidelines

- Only second-generation web authentication and app-based authentication are supported.
- The configured port number must be consistent with the port actually used by the portal server.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the web authentication template configuration mode.

web-auth template { **eportalv2** | *template-name* **v2** | **appauth** }

(4) Configure the communication port of the portal server.

port *port-number*

The default portal server communication port is **50100** for second-generation web authentication and **80** for app-based authentication.

1.10 Configuring the Binding Mode

1.10.1 Overview

The binding mode defines the binding relationship between users and packets and is classified into the IP address binding mode and IP address+MAC address binding mode.

- In IP address binding mode, it is regarded that a packet belongs to a user if the IP address in the packet is the same as that of the user.
- In IP address+MAC address binding mode, it is regarded that a packet belongs to a user only if the IP address and MAC address in the packet are the same as those of the user.

1.10.2 Restrictions and Guidelines

The binding mode is selected based on the user information that the NAS can obtain. If the NAS can obtain a user's IP address and MAC address, the IP address+MAC address binding mode is preferred (such as L2 network deployment). Otherwise, the IP address binding mode is preferred (such as L3 network deployment, in which the NAS cannot obtain users' MAC addresses and can obtain only the gateway's MAC address).

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the web authentication template configuration mode.

web-auth template { **appauth** | **eportalv1** | **eportalv2** | *template-name* { **app** | **v1** | **v2** } }

(4) Configure the binding mode used by a template.

bindmode { **ip-mac-mode** | **ip-only-mode** }

The default binding mode used by a template is IP address+MAC address.

1.11 Configuring the Redirection HTTP Port

1.11.1 Overview

The NAS needs to intercept HTTP packets with specified ports from users and redirect these HTTP packets to the authentication page to complete authentication. The NAS intercepts HTTP packets with destination ports 80 and 443 by default. By configuring the redirection HTTP port, the NAS can intercept HTTP packets with custom ports.

1.11.2 Restrictions and Guidelines

- The commonly used management ports on the access or convergence device, such as ports 22, 23, and 53, and ports reserved by the system are not allowed to be configured as the redirection port.
- HTTP seldom uses ports with numbers smaller than 1000 except port 80. To avoid a conflict with well-known Transmission Control Protocol (TCP) ports, do not configure a port with a small number as the redirection port.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the redirection HTTP port.

http redirect port *port-num*

The NAS intercepts HTTP packets with port numbers 80 and 443 from users and redirects them to the authentication page by default.

A maximum of 10 different destination port numbers can be configured, excluding the default ports 80 and 443.

1.12 Configuring the Redirection Connection Timeout Time

1.12.1 Overview

HTTP redirection is implemented by establishing a TCP connection between the NAS and a user host and adding the redirection page URL to the 302 packet replied by the NAS. After a TCP connection is established between the NAS and a user host, the TCP connection is closed after the NAS receives an HTTP GET/HEAD packet from the user host and responds with an HTTP redirection packet.

The redirection connection timeout time prevents a TCP connection being occupied for a long time because the user host does not send a GET/HEAD packet. After the timeout time expires, the NAS will forcibly disconnect the TCP connection.

1.12.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the redirection connection timeout time.

http redirect timeout *timeout*

The default redirection connection timeout time is **3** seconds.

1.13 Configuring Portal Detection

1.13.1 Overview

The portal detection function periodically detects whether the active portal server is available. When the active portal server is unavailable, the standby server automatically takes over the services.

The portal detection methods vary depending on the web authentication solution. The simple principles are as follows:

- First-generation web authentication: The NAS attempts to establish a connection with the portal server. If the connection can be established, the NAS determines that the portal server is available.
- Second-generation web authentication: The NAS constructs and sends portal packets to the portal server. If the portal server returns response packets, the NAS determines that the portal server is available.

1.13.2 Restrictions and Guidelines

- This function is used when multiple portal servers are deployed. In this case, when the active portal server is unavailable, services are automatically switched to a standby portal server.
- This function can be configured in first-generation and second-generation web authentication. However, the detection method varies depending on the web authentication solution.

1.13.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure portal detection.

web-auth portal-check [**interval** *interval*] [**timeout** *timeout*] [**retransmit** *retransmit-times*]

Portal detection is disabled by default.

1.14 Configuring Portal Escape

1.14.1 Overview

After portal escape is configured, new users are allowed to access network resources without authentication when no portal server is available.

Configure this function if some key services in the network need to be maintained when the portal server is faulty.

1.14.2 Restrictions and Guidelines

- To use this function, you must configure portal detection.
- If multiple portal servers are configured, the escape function takes effect only when all the portal servers are unavailable.
- This function is intended only for the portal server and does not take effect to the RADIUS server.

1.14.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure portal escape.

web-auth portal-escape [**nokick**]

Portal escape is disabled by default.

If the nokick attribute is configured, the system does not force users offline when the escape function takes effect. If the nokick attribute is not configured, the system forces users offline when the escape function takes effect.

1.15 Configuring the Portal Communication Source Port

1.15.1 Overview

After the portal communication source port is configured, the NAS uses the source port to communicate with the portal server, and the used source IP address is the IP address configured on the source port.

1.15.2 Restrictions and Guidelines

Only one portal communication source port can be configured.

1.15.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the portal communication source port.

ip portal source-interface *interface-type interface-num*

No portal communication source port is configured by default.

1.16 Disabling Portal Specification Extension

1.16.1 Overview

Disabling portal specification extension is configured to support different portal servers.

Ruijie second-generation web authentication extends the CMCC WLAN Service Portal Specification. You need to determine whether to use the extension mode based on the server performance. If the portal server is a Ruijie product, enable portal specification extension. If the portal server complies with the CMCC WLAN Service Portal Specification, disable portal specification extension.

1.16.2 Restrictions and Guidelines

- Only second-generation web authentication is supported. When the NAS interworks with a portal server that complies with the CMCC WLAN Service Portal Specification, you can select multiple redirection URL formats to achieve compatibility with different servers.

1.16.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable portal specification extension.

no web-auth portal extension

Portal specification extension is enabled by default.

1.17 Configuring Transparent Transmission of RADIUS Private Attributes

1.17.1 Overview

After transparent transmission of RADIUS private attributes is enabled, the web authentication module uploads the private attributes delivered by the portal server to the RADIUS server and transparently transmits Ruijie private attributes in RADIUS authentication results to the portal server.

1.17.2 Restrictions and Guidelines

This function is used only on Ruijie Serverless Application Model (SAM) servers and portal servers. If the NAS interworks with a portal server provided by other vendors, you are not advised to enable this function. If this function is enabled, the portal server may not respond to packets.

1.17.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure transparent transmission of RADIUS private attributes.

web-auth portal-import attr-26

Transparent transmission of RADIUS private attributes is disabled by default.

1.18 Configuring the Authentication-Free Network Resource Range

1.18.1 Overview

Authentication-free network resources allow user access without authentication.

After web authentication or 802.1X authentication is enabled on a port, the user hosts connecting to the port need to pass authentication before accessing network resources. After the authentication-free network resource range is configured, unauthenticated users can access resources within the range without authentication.

1.18.2 Restrictions and Guidelines

The number of authentication-free network resources and the number of authentication-exempted users cannot exceed 1000. The actual number of available resources may be reduced because of other security modules. Therefore, it is recommended that network segments be configured if many addresses need to be configured.

1.18.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the authentication-free network resource range.

http redirect direct-site *ipv4-address* [*mask*] [**arp** | *port-number*&<1-8>]

No authentication-free network resource range is configured by default.

1.19 Configuring a Straight-through ARP Resource Range

1.19.1 Overview

You can configure a straight-through Address Resolution Protocol (ARP) resource range to permit the ARP packets from the specified address to pass.

When ARP check or a similar function is enabled, users cannot learn the ARP entries of the gateway or other devices, which affects user experience. You can configure this function to ensure normal ARP learning.

1.19.2 Restrictions and Guidelines

- When ARP check is enabled, you need to configure the gateway of the PCs connecting to the L2 access device as a straight-through ARP resource. If both straight-through websites and ARP resources are configured for the same address/network segment, the commands will be combined automatically. If no ARP option is specified in the straight-through website configuration, the option will be added automatically after combination.
- When ARP check is enabled, if the outbound interface address of the PC connecting to the L2 access device is not the gateway address, you need to configure the outbound interface address as a straight-through ARP resource. If multiple outbound addresses exist, configure these addresses as straight-through ARP resources.
- If ARP check is enabled, you must configure the authentication-free network resources and gateway address as straight-through ARP resources.

1.19.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a straight-through ARP resource range.

http redirect direct-arp { *ipv4-address* [*mask*] }

No straight-through ARP resource range is configured by default.

1.20 Configuring an Authentication-Exempted User Range

1.20.1 Overview

After an authentication-exempted user range is configured, users within the range can access all reachable network resources without authentication. The authentication-exempted user range can be defined by IP address and MAC address.

The authentication-exempted user range can be used to allow special user groups that do not need permission control to access network resources.

1.20.2 Restrictions and Guidelines

The number of authentication-exempted users and the number of authentication-free network resources cannot exceed 1000. The actual number of available resources may be reduced because of other security modules. Therefore, it is recommended that network segments be configured if many addresses need to be configured.

1.20.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an authentication-exempted user range. Configure at least one of the tasks.

- Configure the IP address range of users who do not require authentication.

  web-auth direct-host { *ipv4-address* [*ipv4-mask* | **arp**] }

- Configure the MAC address range of users who do not require authentication.

  web-auth direct-host *mac-address*

No IP/MAC address range of authentication-exempted users is configured by default. All users can access restricted network resources only after they pass web authentication.

1.21 Configuring Logging of the Web Authentication Module

1.21.1 Overview

The logging function of the web authentication module can send log messages to the administrator to display the information and relevant events of users who get online/offline and allow users to configure a log printing rate limit.

1.21.2 Restrictions and Guidelines

When the online/offline rate is high, you can configure a rate limit for log printing. This prevents frequent log output from affecting the device performance and resulting in spamming.

1.21.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure web authentication logging.

web-auth logging enable *log-rate*

The web authentication logging function is disabled by default.

1.22 Configuring the Maximum Number of HTTP Sessions for Unauthenticated Users

1.22.1 Overview

When an unauthenticated user accesses network resources, the user's PC sends requests for HTTP session connection. The access or convergence device intercepts the HTTP packets and redirects the user to a web authentication page. To prevent an unauthenticated user from initiating too many HTTP connection requests and save resources on the NAS, you need to limit the maximum number of HTTP sessions that the unauthenticated users can initiate on the NAS.

1.22.2 Restrictions and Guidelines

- User authentication occupies one HTTP session, and other applications of a user may also need HTTP sessions. Therefore, you are not advised to set the maximum number of HTTP sessions to 1 for unauthenticated users.
- If the authentication page fails to be displayed during web authentication, the maximum number of HTTP sessions may be reached. When this happens, the user can close the application programs that occupy HTTP sessions and perform web authentication again.

1.22.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of HTTP sessions allowed for an unauthenticated user.

http redirect session-limit *session-number*

The maximum number of HTTP sessions allowed for an unauthenticated user is **255** by default.

1.23 Configuring the Interval for Updating Online User Information

1.23.1 Overview

The NAS needs to periodically update maintained online user information, for example, the online time. The interval for updating online user information can be manually configured based on different monitoring requirements for online user information in different scenarios.

1.23.2 Restrictions and Guidelines

The interval for updating online user information must be a multiple of 60. If the configured value is not a multiple of 60, the actual effective value is rounded up to the multiple of 60.

1.23.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the interval for updating online user information.

web-auth update-interval *update-interval*

The default interval for updating online user information is **180** seconds.

1.24 Enabling DHCP Address Check

1.24.1 Overview

After Dynamic Host Configuration Protocol (DHCP) address check is configured, authentication is performed only for addresses assigned through DHCP. This function can be configured in global and interface configuration modes based on actual requirements.

1.24.2 Restrictions and Guidelines

- To use this function, you must configure DHCP Snooping.
- Only second-generation web authentication is supported for users with IPv4 addresses.
- This function applies only to network environments with IP addresses assigned through DHCP. If users with statically configured IP addresses exist, network access of these users will be limited.
- If only a few users need to use static IP addresses, configure these IP addresses as straight-through addresses. In this case, these users are exempted from authentication.
- To apply this function to an interface, disable global DHCP address check first.

1.24.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure DHCP address check. Configure at least one of the tasks.

- Enable DHCP address check globally.

  web-auth dhcp-check

  DHCP address check is disabled globally by default.

- Enable DHCP address check on an interface. Run the following commands in sequence:

  interface *interface-type interface-number*

  web-auth dhcp-check vlan vlan-list

  DHCP address check is disabled on an interface by default.

(4) (Optional) Disable DHCP address check on a VLAN.

web-auth dhcp-check vlan disable

DHCP address check is enabled on a VLAN by default.

1.25 Configuring an Address Whitelist

1.25.1 Overview

After an address whitelist is configured, users can access some network resources before authentication.

1.25.2 Restrictions and Guidelines

- A whitelist can contain a maximum of 1000 addresses.
- When whitelisted addresses are configured in domain name format, you need to configure the domain name server (DNS) function for the NAS to enable the NAS to correctly parse domain names.
- Some domain names correspond to multiple IP addresses. A domain name can map to eight IP addresses at most.

1.25.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an address whitelist.

web-auth acl [**oob** | **vrf** *vrf-name*] **white-url** *white-url-name*

No whitelist is configured by default.

1.26 Configuring VLAN-based Authentication on a Port

1.26.1 Overview

After VLAN-based authentication is configured on a port, only the user hosts in the configured VLAN can initiate web authentication.

1.26.2 Restrictions and Guidelines

When this function is configured, multiple VLANs can be specified.

1.26.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure VLAN-based authentication on a port.

web-auth vlan-control *vlan-list*

VLAN-based authentication is not configured on a port by default. Port-based authentication is used by default.

1.27 Configuring the Authenticated User Logout Delay on a Port

1.27.1 Overview

After the authenticated user logout delay is configured on a port, the user hosts connected to the port go offline after the delay when the port is down.

1.27.2 Restrictions and Guidelines

You are advised to configure this function to prevent repeated user authentication in scenarios when a port goes down and then up quickly.

1.27.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the authenticated user logout delay after a port is down.

web-auth linkdown-timeout *linkdown-timeout*

The default authenticated user logout delay after a port is down is **60** seconds.

1.28 Enabling RADIUS Server Escape

1.28.1 Overview

After the RADIUS server escape function is configured, users can still perform authentication to access the Internet when the RADIUS server fails.

1.28.2 Restrictions and Guidelines

This function must be used together with RADIUS server detection function. For details about the RADIUS server detection command, see "Configuring RADIUS" in the *Security Configuration Guide*.

1.28.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable RADIUS server escape.

web-auth radius-escape

The RADIUS server escape function is disabled by default.

1.29 Configuring DHCP Server Detection

1.29.1 Overview

DHCP server detection can find offline web authentication users in a DHCP environment in time, ensuring accurate accounting.

In a network environment where IP addresses are dynamically assigned through DHCP, a DHCP client can send a DHCP RELEASE packet to proactively release the IP address assigned by the DHCP server. The DHCP client without an IP address cannot access the network. If the DHCP server detection function is enabled, the NAS with DHCP Server and web authentication enabled will force the corresponding authenticated user offline when receiving a DHCP RELEASE packet from the DHCP client. If the DHCP server detection function is disabled, the NAS will not force the corresponding authenticated user offline in the preceding scenario.

1.29.2 Restrictions and Guidelines

- The DHCP server detection function is enabled by default.
- This function applies only to network environments with DHCP deployed and takes effect only when both DHCP server and web authentication are enabled on the device.

1.29.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable DHCP server detection.

no web-auth dhcp-server check

The DHCP server detection function is enabled by default.

1.30 Configuring Uniqueness Check of Portal Authentication Accounts

1.30.1 Overview

After uniqueness check of portal authentication accounts is enabled, the NAS returns an ACK_AUTH message carrying Errcode 2 to the portal server if account information of a new authenticated user is being used by an online user. Upon receiving such a reply message, some portal servers will send the "Terminal Preemption" prompt to users.

1.30.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable uniqueness check of portal authentication accounts.

web-auth portal-valid unique-name

Uniqueness check of portal authentication accounts is disabled by default.

1.31 Enabling Automatic Adding of Domain Information After Usernames

1.31.1 Overview

After automatic adding of domain information after usernames is enabled, the web authentication module will automatically add configured domain information after the original usernames and use the new usernames for authentication.

1.31.2 Restrictions and Guidelines

- The domain information can be 63 bytes at most.
- The new username is obtained by adding configured domain information after the username sent by the portal server. If the new username exceeds 253 bytes, the excess of domain information will be intercepted.

1.31.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the web authentication template configuration mode.

web-auth template { **appauth** | **eportalv1** | **eportalv2** | *template-name* **app** | *template-name* **v1** | *template-name* **v2** }

(4) Enable automatic adding of domain information after usernames.

domain *domain-info*

No domain information is added after usernames by default.

1.32 Configuring HTTPS Certificate Import

1.32.1 Overview

HTTPS is an encrypted data transmission protocol and relies on a certificate to ensure transmission security. Before enabling the HTTPS server function, you need to import an available certificate.

To configure HTTPS certificate import, first upload available HTTPS certificate and key files to the NAS and then apply the HTTPS certificate and key files.

1.32.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Upload the HTTPS certificate and key files.

web-auth import-ssl { **cert ftp:***path* | **cert tftp:***path* | **cert oob_ftp:***path* | **cert oob_tftp:***path* } { **key ftp:***path* | **key tftp:***path* | **key oob_ftp:***path* | **key oob_tftp:***path* } [**vrf** *vrf-name*]

(3) Apply the HTTPS certificate and key files.

web-auth ssl-policy https-redirect

No HTTPS certificate or key file is applied by default.

1.33 Enabling Adding the Authentication Page to Favorite

1.33.1 Overview

After the function of adding the authentication page to Favorite is enabled, a user can add the authentication page to Favorite and open the Favorite page for web authentication without needing redirection.

1.33.2 Restrictions and Guidelines

- This function must be used together with DHCP Snooping.
- This function cannot be configured with 802.1x authentication simultaneously. Otherwise, a user may be online for web authentication and 802.1x authentication at the same time.

1.33.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of adding the authentication page to Favorite.

web-auth portal direct-auth

The function of adding the authentication page to Favorite is disabled by default.

1.34 Configuring a Template Mapping Method

1.34.1 Overview

The template mapping method is configured when multiple authentication scenarios exist on one port.

When web authentication is enabled on a port, and the method of template A is used, but some users do not apply to template A and want to use template B for authentication, you can configure a template mapping method for these users to enable these users to use the authentication method of template B.

1.34.2 Restrictions and Guidelines

By setting the VLAN or IP address range, you can select users for whom a template mapping method needs to be configured.

1.34.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a template mapping method, and determine the user range and the corresponding authentication template method.

web-auth mapping *mapping-method* { **vlan** *vlan-list* | **ip-mapping** *ipv4-address ipv4-mask* } **template** *tmpltate-name*

No template mapping method is configured by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Apply the template mapping method.

web-auth apply-mapping *mapping-method*

No template mapping method is applied on an interface by default.

1.35 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Notice

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

Table 1-2 Monitoring

Command	Purpose
show web-auth acl [**white-url** | **white-port**]	Displays whitelist configurations.
show web-auth authmng [**statistic** | **abnormal**]	Displays the web authentication data.
show web-auth parameter	Displays basic parameter configurations for web authentication.
show web-auth control	Displays authentication control configuration.
show web-auth direct-arp	Displays the straight-through ARP resource range.
show web-auth direct-host	Displays the authentication-exempted user range.
show web-auth direct-site	Displays the straight-through website range.
show web-auth ip-mapping	Displays the configured mapping between servers and users.
show web-auth portal-check	Displays portal-check parameters.
show web-auth rdport	Displays the TCP interception port.
show web-auth syslog ip *ip-address*	Displays user online and offline records.
show web-auth template	Displays portal server configurations.
show web-auth user { **all** | **ip** *ipv4-address* | **mac** *mac-address* | **name** *name* }	Displays user online information.
clear web-auth acl white-url	Clears web authentication whitelist configurations.
clear web-auth direct-arp	Clears all ARP resources.
clear web-auth direct-host	Clears all authentication-exempted users.
clear web-auth direct-site	Clears all authentication-free network resources.
clear web-auth user { **all** | **id** *num* | **ip** *ipv4-address* | **mac** *mac-address* | **name** *name* }	Forces users offline.
debug web-auth all	Debugs web authentication.

1.36 Configuration Examples

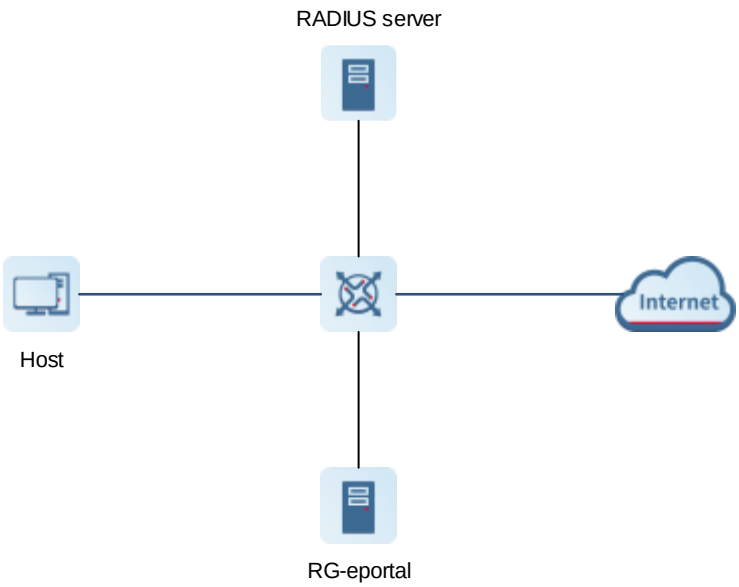
1.36.1 Configuring First-Generation Web Authentication

1. Requirements

The NAS serves as the network access server (NAS) and enables first-generation web authentication for user hosts connecting to a specified port. These user hosts can access the network only after authentication by using valid accounts and passwords.

2. Topology

Figure 1-5 Configuring First-Generation Web Authentication



3. Notes

- Configure the portal server to support first-generation web authentication.
- Configure the RADIUS server to support first-generation web authentication.
- Configure the first-generation web authentication template and specify the portal server IP address, redirection page, and other parameters.
- Configure the communication key between the NAS and the portal server.
- Configure SNMP parameters between the NAS and the portal server.
- Enable first-generation web authentication on a port of the NAS.

4. Procedure

(1) Configure the portal server and RADIUS server to support first-generation web authentication. For details about the configuration procedure, see the corresponding configuration guide.

(2) Configure the first-generation web authentication template and set the portal server IP address to 192.168.1.3 and redirection page URL to http://192.168.1.3/eportal/index.jsp.

```
Device> enable
Device# configure terminal
```

```
Device(config)# web-auth template eportalv1
Device(config.tmplt.eportalv1)# ip 192.168.1.3
Device(config.tmplt.eportalv1)# url http://192.168.1.3/eportal/index.jsp
Device(config.tmplt.eportalv1)# exit
```

(3) Set the communication key between the NAS and the portal server to key_1 (which must be the same as that configured on the portal server).

```
Device(config)# web-auth portal key key_1
```

(4) Enable the SNMPv2 function.

```
Device(config)# enable service snmp-agent
Device(config)# snmp-server enable version v2c
```

(5) Configure SNMP community string community_1 and enable the SNMP trap/inform function. The SNMP server address is the portal server address.

```
Device(config)# snmp-server community community_1 rw
Device(config)# snmp-server host 192.168.1.3 inform version 2c community_1
web-auth
Device(config)# snmp-server enable traps web-auth
```

(6) Enable first-generation web authentication on GigabitEthernet 0/2 and GigabitEthernet 0/3.

```
Device(config)#int range gigabitEthernet 0/2-3
Device(config-if-range)#web-auth enable eportalv1
```

5. Verification

Check that first-generation web authentication takes effect on GigabitEthernet 0/2 and GigabitEthernet 0/3.

```
Device# show web-auth control
 Port                    Control  Server Name    Online User Count Arp-detect Vlan
Control List
 ------------------------- -------- -------------------------------- ------------
----- ----------
 GigabitEthernet 0/2      On      eportalv1      0               Off
 GigabitEthernet 0/3      On      eportalv1      0               Off
```

Check that parameters of the web authentication template are correctly configured.

```
Device# show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:             eportalv1
  BindMode:          ip-only-mode
  Type:             v1
  Ip:               192.168.1.3
  Url:              http://192.168.1.3/eportal/index.jsp
```

When user hosts connecting to GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS access a webpage, the hosts will be redirected to http://192.168.1.3/eportal/index.jsp for authentication. The hosts can access the network after they pass authentication.

6. Configuration Files

```
!
web-auth template eportalv1
 ip 192.168.1.3
 url 192.168.1.3/eportal/index.jsp
!
web-auth portal key key_1
!
enable service snmp-agent
!
snmp-server host 192.168.1.3 informs version 2c 7 $10$255$lxTDxZBSy7ToI2s=$ web-
auth
snmp-server enable traps web-auth
snmp-server enable version v2c
snmp-server community 7 $10$255$lxTDxZBSy7ToI2s=$ rw
!
interface GigabitEthernet 0/2
 web-auth enable eportalv1
!
interface GigabitEthernet 0/3
 web-auth enable eportalv1
!
```

7. Common Errors

- The SNMP parameters used for the communication between the portal server and the NAS are configured incorrectly, causing authentication failures.
- When web authentication is deployed on L3 networks, **ip-only-mode** is not selected as the binding mode in the template.
- When web authentication is used together with Virtual Router Redundancy Protocol (VRRP), the **snmp-server trap-source ip** command is not configured to specify the VRRP address. As a result, the portal server cannot process Trap packets correctly.

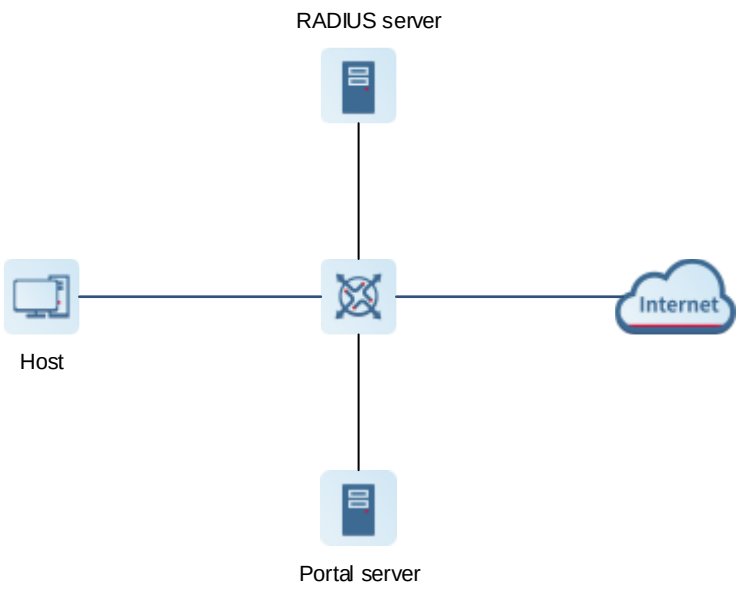
1.36.2 Configuring Second-Generation Web Authentication

1. Requirements

The NAS serves as the NAS and enables second-generation web authentication for user hosts connecting to a specified port. These user hosts can access the network only after authentication by using valid accounts and passwords.

2. Topology

Figure 1-6 Configuring Second-Generation Web Authentication



3. Notes

- Configure the portal server to support second-generation web authentication.
- Configure the RADIUS server to support second-generation web authentication.
- Enable AAA security services on the device.
- Configure the IP address and communication key of the RADIUS server.
- Configure the default web authentication and accounting method lists for the AAA module.
- Configure the key used to communicate with the portal server.
- Configure the second-generation web authentication template.
- Enable second-generation web authentication on a port of the NAS.

4. Procedure

(1) Configure the portal server and RADIUS server to support second-generation web authentication. For details about the configuration procedure, see the corresponding configuration guide.

(2) Configure the second-generation web authentication template and set the portal server IP address to 192.168.1.3 and redirection page URL to http://192.168.1.3/eportal/index.jsp.

```
Device> enable
Device# configure terminal
Device(config)# web-auth template eportalv2
Device(config.tmplt.eportalv2)# ip 192.168.1.3
Device(config.tmplt.eportalv2)# url http://192.168.1.3/eportal/index.jsp
Device(config.tmplt.eportalv2)# exit
```

(3) Set the communication key between the NAS and the portal server to key_1 (which must be the same as that configured on the portal server).

```
Device(config)# web-auth portal key key_1
```

(4) Configure the IP address and communication key of the RADIUS server.

```
Device(config)# radius-server host 192.168.1.4 key radiuskey
```

(5) Enable AAA security services.

```
Device(config)# aaa new-model
```

(6) Configure the default web authentication and accounting method lists for the AAA module.

```
Device(config)# aaa authentication web-auth default group radius
Device(config)# aaa accounting network default start-stop group radius
```

(7) Enable second-generation web authentication on GigabitEthernet 0/2 and GigabitEthernet 0/3.

```
Device(config)#int range gigabitEthernet 0/2-3
Device(config-if-range)#web-auth enable eportalv2
```

5. Verification

Check that second-generation web authentication takes effect on GigabitEthernet 0/2 and GigabitEthernet 0/3.

```
Device# show web-auth control
 Port                    Control  Server Name    Online User Count Arp-detect Vlan
Control List
 ------------------------- -------- ------------------------------- ------------
----- ----------
 GigabitEthernet 0/2      On      eportalv2      0               Off
 GigabitEthernet 0/3      On      eportalv2      0               Off
```

Check that parameters of the second-generation authentication template are correctly configured.

```
Ruijie#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:             eportalv2
  BindMode:          ip-mac-mode
  Type:             v2
  Port:             50100
  vrf:
  Ip:               192.168.1.3
  Url:              http://192.168.1.3/eportal/index.jsp
  Authentication:
  Accounting:
  Portal-State:      Enable
  Radius-State:      Enable
```

When user hosts connecting to GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS access a webpage, the hosts will be redirected to http://192.168.1.3/eportal/index.jsp for authentication. The hosts can access the network after they pass authentication.

6. Configuration Files

```
!
web-auth template eportalv2
 ip 192.168.1.3
```

```
 url 192.168.1.3/eportal/index.jsp
!
web-auth portal key key_1
!
aaa new-model
!
aaa accounting network default start-stop group radius
aaa authentication web-auth default group radius
!
radius-server host 172.26.147.194 key 7 $10$3ed$f/3upXnVEhd9$
!
interface GigabitEthernet 0/2
 web-auth enable eportalv2
!
interface GigabitEthernet 0/3
 web-auth enable eportalv2
!
```

7. Common Errors

- The communication key between the portal server and NAS is configured incorrectly, or is configured only on the portal server or NAS, causing authentication errors.
- The communication parameters between the RADIUS server and the NAS are set incorrectly, causing authentication errors.
- The portal server does not support the CMCC WLAN Service Portal Specification, causing a compatibility failure.

Contents

1 Configuring the SCC 1

1.1 Overview 1

1.2 Configuration Task Summary 1

1.3 Configuring Authentication-Exempted VLANs 1

1.3.1 Overview 1

1.3.2 Restrictions and Guidelines 1

1.3.3 Procedure 1

1.4 Configuring the IPv4 User Capacity 2

1.4.1 Overview 2

1.4.2 Restrictions and Guidelines 2

1.4.3 Procedure 2

1.5 Configuring Authenticated User Migration 2

1.5.1 Overview 2

1.5.2 Restrictions and Guidelines 3

1.5.3 Procedure 3

1.6 Monitoring 3

1 Configuring the SCC

1.1 Overview

The Security Control Center (SCC) provides common configuration methods and policy integration for various access control and network security services, so that these services can coexist on one device to meet diversified access and security control requirements in various scenarios.

Typical access control services include 802.1x, web authentication, Address Resolution Protocol (ARP) check, and IP source guard, and typical network security services include access control list (ACL), NFPP, and gateway-targeted ARP spoofing prevention. When two or more access control or network security services are enabled on the same device, the SCC coordinates coexistence based on related policies.

1.2 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring Authentication-Exempted VLANs
- Configuring the IPv4 User Capacity
- Configuring Authenticated User Migration

1.3 Configuring Authentication-Exempted VLANs

1.3.1 Overview

After an authentication-exempted virtual local area network (VLAN) is configured, users in this VLAN can access the Internet without 802.1x or web authentication. When the device detects that a received packet is destined for an authentication-exempted VLAN, the device skips authentication.

The authentication-exempted VLAN function aims to provide easy and convenient network access experience for special groups in networks that require authentication. For example, the headmaster's office in a campus network is configured to be within an authentication-exempted VLAN to ensure network access without authentication.

1.3.2 Restrictions and Guidelines

- When an authentication-exempted VLAN is configured, ensure that the ACL also permits the VLAN. The authentication-exempted VLAN function exempts user packets only from authentication detection. User packets still need to undergo ACL detection. If a specified user or VLAN is denied in the ACL, the specified user or users in the specified VLAN cannot access the Internet.
- A maximum of 100 authentication-exempted VLANs can be configured.
- Configuring authentication-exempted VLANs occupies system resources. If access authentication is disabled on a device, the authentication-exempted VLAN function is meaningless and needs to be disabled.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure authentication-exempted VLANs.

direct-vlan *vlan-list*

No authentication-exempted VLAN is configured by default.

1.4 Configuring the IPv4 User Capacity

1.4.1 Overview

The IPv4 user capacity is used to limit the maximum number of IPv4 access users on a port of the device. When the total number of IPv4 access users on a port reaches the limit, new users cannot access the network over this port. You need to select a proper user capacity based on the actual environment to guard against brutal force impacts from unauthorized users and improve the operational stability of the device.

1.4.2 Restrictions and Guidelines

IPv4 users include those generated through 802.1x authentication, web authentication, and other binding functions. IPv4 users on a port may be generated over the port or globally. For example, when a global IPv4 user is bound to a port by running the corresponding command, the user is also calculated as a user on the port.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the IPv4 user capacity on a port.

nac-author-user maximum *max-user-number*

The IPv4 user capacity on a port is not limited by default.

1.5 Configuring Authenticated User Migration

1.5.1 Overview

In actual scenarios, access users usually pass authentication and get online through one physical location, and then switch to another physical location for office or entertainment. For example, an enterprise employee takes a tablet from one office to another office to access the Internet by directly removing the network cable instead of getting offline proactively. If the authenticated user migration function is not configured, the employee cannot pass authentication to access the Internet in the other office because the original account does not get offline.

By default, 802.1x and web authentication users cannot switch from one physical location (access port+VLAN) to another to perform authentication and access the Internet again if they do not get offline. The authenticated user migration function allows users to realize this.

When authenticated user migration is enabled, the 802.1x or web authentication module of the device detects that the port or VLAN corresponding to a user's media access control (MAC) address has changed. Then, the user is forced offline and needs to be authenticated again before getting online. This prevents malicious users from forging online users' MAC addresses to access the Internet and causing authenticated users being forced offline. The authenticated user migration function determines the MAC address authenticity. For a user who gets online through web authentication or 802.1x authentication with IP authorization, the 802.1x or web authentication module sends an ARP request to the original physical location of the user if detecting that the same MAC address is online in another VLAN or on another port. If no response is received within the specified time, the module determines that the user's location has changed and the migration is allowed.

1.5.2 Restrictions and Guidelines

- The authenticated user migration function requires a check of users' MAC addresses, and is invalid for users who have IP addresses only.
- When both 802.1x authentication and port security are enabled on a port, and port security and 802.1x authentication users get online simultaneously, 802.1x authenticated users will fail to be migrated to another port to get online because the same MAC address cannot go online through different ports.
- The user online detection function can kick users offline. When the authentication user migration function is not configured and a user does not proactively get offline, the user may be kicked offline by the online detection function and can implement authentication and get online in another physical location.
- When an online authenticated user moves to a new physical location, the user needs to perform 802.1x or web authentication again.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable authenticated user migration.

station-move permit

Authenticated user migration is disabled by default.

1.6 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** commands to output debugging information.

Notice

The output debugging information occupies system resources. Therefore, disable the debugging switch immediately after use.

Table 1-1 Monitoring

Command	Purpose
show direct-vlan	Displays authentication-exempted VLAN configurations.
show nac-author-user [**interface** *interface-type interface-number*]	Displays IPv4 user entries on a port.
show access-control packet statistics [**interface** *interface-type interface-number* | **vlan** *vlan-id*]	Displays statistics about packets filtered due to access control.
debug scc event	Debugs the SCC running process.
debug scc user	Debugs SCC user entries.
debug scc acl-show summary	Debugs ACL summary stored in the SCC delivered by various services.
debug scc acl-show all	Debugs all ACLs stored in the SCC.

Contents

1 Configuring Password Policies 1
1.1 Introduction 1
1.1.1 Overview 1
1.2 Restrictions and Guidelines 1
1.3 Configuration Task Summary 1
1.4 Configuring the Minimum Password Length 1
1.4.1 Overview 1
1.4.2 Procedure 1
1.5 Enabling Strong Password Detection 2
1.5.1 Overview 2
1.5.2 Procedure 2
1.6 Enabling Forcible Weak Password Change 2
1.6.1 Overview 2
1.6.2 Procedure 2
1.7 Configuring a Password Lifecycle 3
1.7.1 Overview 3
1.7.2 Procedure 3
1.8 Configuring Repeated Password Use Prevention 3
1.8.1 Overview 3
1.8.2 Procedure 3
1.9 Configuring Encrypted Password Storage 4
1.9.1 Overview 4
1.9.2 Procedure 4

1.10 Enabling Special Character Detection....4

1.10.1 Overview....4

1.10.2 Procedure....4

1.11 Monitoring....4

1.12 Configuration Examples....5

1.12.1 Requirements....5

1.12.2 Topology....5

1.12.3 Notes....5

1.12.4 Procedure....5

1.12.5 Verification....6

1.12.6 Configuration Files....6

1 Configuring Password Policies

1.1 Introduction

1.1.1 Overview

A password policy provides the password detection function for applications that need to configure accounts and passwords (for example, creating local users) on a device to ensure that users use passwords that meet security specifications and prevent password crackdown due to low password complexity.

1.2 Restrictions and Guidelines

The password lifecycle, repeated password use prevention, and forcible weak password change functions take effect only to global passwords (**enable password** and **enable secret**) and local user passwords (**username** *username* **password** *password*) and are invalid to passwords in line configuration mode.

1.3 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

(1) Configuring the Minimum Password Length

(2) Enabling Strong Password Detection

(3) Enabling Forcible Weak Password Change

(4) Configuring a Password Lifecycle

(5) Configuring Repeated Password Use Prevention

(6) Configuring Encrypted Password Storage

(7) Enabling Special Character Detection

1.4 Configuring the Minimum Password Length

1.4.1 Overview

The minimum password length is used to limit the length of user passwords.

If the password entered by a user is shorter than the minimum password length, the system displays an error prompt, asking the user to specify another password of an appropriate length.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the minimum password length.

password policy min-size *min-size*

No minimum length is configured for passwords by default.

1.5 Enabling Strong Password Detection

1.5.1 Overview

Strong password detection is used to detect the complexity of a password and prevent password crackdown due to low complexity.

The strong password detection function will send an alarm and disallow the user to configure the password in the following scenarios:

- The password is the same as the corresponding account.
- The password contains only digits.
- The password contains only uppercase letters.
- The password contains only lowercase letters.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the strong password detection function.

password policy strong

The strong password detection function is enabled by default.

1.6 Enabling Forcible Weak Password Change

1.6.1 Overview

The forcible weak password change function is used together with another password policy (such as the minimum password length or strong password detection).

After the forcible weak password change function is enabled, a warning prompt will be displayed if a user uses a weak password (containing less than 8 bytes or only digits, uppercase letters, or lowercase letters) during login or configuration.

If both the forcible weak password change function and another password policy are enabled, the password will continue to be checked according to the other password policy during user login. If the password does not meet requirements of the other password policy, a prompt for changing the password will be displayed. The user is allowed to log in only after the new password meets requirements of the password policy.

1.6.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable forcible weak password change.

password policy forced-password-modify

Forcible weak password change is disabled by default.

1.7 Configuring a Password Lifecycle

1.7.1 Overview

The password lifecycle defines the validity time of a password.

If a user enters a password that has already expired during login, the system gives a prompt, indicating that the password has expired, and asks the user to reset the password.

1.7.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the password lifecycle.

password policy life-cycle *life-cycle*

No password lifecycle is configured by default.

1.8 Configuring Repeated Password Use Prevention

1.8.1 Overview

The repeated password use prevention function prevents users from using historically configured passwords as new passwords.

The system records passwords used by a user to a historical password list. If a newly configured password is within the list, the system gives a prompt and asks the user to specify another password. The maximum number of records in the password list can be manually configured. When the number of records in the password list reaches the limit, a new password record will overwrite the earliest password record.

1.8.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Prevent repeated use of passwords configured in the latest specified number of times.

password policy no-repeat-times *no-repeat-times*

Repeated password use is allowed by default.

1.9 Configuring Encrypted Password Storage

1.9.1 Overview

Encrypted password storage is used to store passwords after encryption.

When administrators run the **show running-config** command to display configurations or run the **write** command to save configuration files, passwords configured by users are displayed in ciphertext format if encrypted password storage is enabled and displayed in plaintext format if encrypted password storage is disabled.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable encrypted password storage.

service password-encryption

Encrypted password storage is disabled by default.

1.10 Enabling Special Character Detection

1.10.1 Overview

After strong password detection and special character detection are configured, passwords that contain only special characters are invalid and cannot be configured successfully. Special characters include space, tilde (~), backtick (`), exclamation mark (!), at sign (@), number sign (#), dollar sign ($), percent sign (%), caret (^), ampersand (&), asterisk (*), brackets (()), underscore (_), plus sign (+), minus sign (–), equal sign (=), braces ({}), vertical bar (|), square brackets ([]), backslash (\), colon (:), quotation mark ("), semicolon (;), apostrophe ('), angle brackets (<>), comma (,), period (.), and slash (/).

1.10.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable special character detection.

password policy printable-character-check

Special character detection is disabled by default.

1.11 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show password policy	Displays configured password security policies.

1.12 Configuration Examples

1.12.1 Requirements

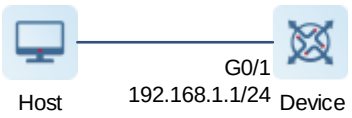
To ensure password complexity, you can configure password policies on a device to limit users' passwords.

Password security requirements are as follows:

- A password must be a string of at least eight characters.
- A password cannot be the same as the account.
- A password cannot contain only digits, uppercase letters, or lowercase letters.
- A password is valid for 90 days.
- Passwords must be stored in encrypted mode.
- A password cannot be the same as historical passwords configured in the latest three times.

1.12.2 Topology

Figure 1-1 Configuring Password Policies



1.12.3 Notes

- Set the minimum password length to 8.
- Enable strong password detection.
- Set the password lifecycle to 90 days.
- Enable encrypted password storage.
- Configure repeated password use prevention to disable the use of historical passwords configured in the latest three times.

1.12.4 Procedure

Enter the global configuration mode.

```
Device> enable
Device# configure terminal
```

Set the minimum password length to 8.

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

Enable strong password detection.

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

Set the password lifecycle to 90 days.

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

Enable encrypted password storage.

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

Configure repeated password use prevention to disable the use of historical passwords configured in the latest three times.

```
Device(config)# password policy no-repeat-times 3
```

1.12.5 Verification

Run the **show password policy** command to display configured password policies.

```
Device> enable
Device# show password policy
Global password policy configurations:
 Password encryption:              Enabled
 Password strong-check:            Enabled
 Password forced-password-modify:    Disabled
 Password min-size:                Enabled (8 characters)
 Password life-cycle:              Enabled (90 days)
 Password no-repeat-times:          Enabled (max history record: 3)
 Password printable-character-check:  Disabled
```

1.12.6 Configuration Files

```
!
password policy life-cycle 90
password policy no-repeat-times 3
password policy min-size 8
password policy strong
service password-encryption
```

Contents

1 Configuring SSH....1
1.1 Introduction....1
1.1.1 Overview....1
1.1.2 Principles....1
1.1.3 Protocols and Standards....3
1.2 Configuration Task Summary....3
1.3 Configuring SSH Server....4
1.3.1 Overview....4
1.3.2 Configuration Tasks....4
1.3.3 Enabling SSH Server....4
1.3.4 Configuring the SSH Server Version....5
1.3.5 Configuring the Listening Port....5
1.3.6 Configuring the Key and Key Exchange Algorithm of the SSH Server....6
1.3.7 Configuring the Encryption Algorithm....6
1.3.8 Configuring Authentication Parameters....7
1.3.9 Configuring an ACL....7
1.3.10 Configuring IP Address Blocking....8
1.3.11 Disconnecting an SSH Client Connection....8
1.4 Configuring SCP Server....9
1.4.1 Overview....9
1.4.2 Restrictions and Guidelines....9
1.4.3 Procedure....9
1.5 Configuring SSH Client....9

1.5.1 Overview 9

1.5.2 Configuration Tasks 9

1.5.3 Establishing a Connection with the SSH Server 10

1.5.4 Restoring an Established SSH Client Session 10

1.5.5 Disconnecting a Suspended SSH Client Session 11

1.6 Configuring SCP Client 11

1.6.1 Overview 11

1.6.2 Procedure 11

1.7 Monitoring 11

1.8 Configuration Examples 12

1.8.1 Configuring Line Password Authentication for SSH Users 12

1.8.2 Configuring Local User Authentication for SSH Clients 14

1.8.3 Configuring AAA Authentication for SSH Clients 16

1.8.4 Configuring Public Key Authentication for SSH Clients 18

1.8.5 Configuring SCP Server 19

1.8.6 Configuring SSH Client 21

1.8.7 Configuring SCP Client 22

1 Configuring SSH

1.1 Introduction

1.1.1 Overview

Secure Shell (SSH) is a network security protocol that requires encryption and authentication and is used for remote access and file transfer.

SSH is based on the server/client structure. The device supports both the SSH server and client functions. As an SSH server, the device can connect to multiple SSH clients. As an SSH client, the device allows users to establish SSH connections with devices that support the SSH server function.

The SSH function is similar to the Telnet service. However, the encryption and authentication features of SSH can ensure stronger security guarantee for users. When users log in to the device through an insecure network environment, SSH can effectively protect the device against attacks, such as IP address spoofing and plaintext password interception.

1.1.2 Principles

1. SSH Version

SSHv1 and SSHv2 are available, and the two are mutually exclusive. Compared with SSHv1, SSHv2 provides higher performance and security.

The device supports both versions and supports SSH interaction using the IPv4 and IPv6 addresses. Unless otherwise specified, SSH in this document refers to SSHv2.

2. SSH Exchange Process

Interaction between an SSH client and an SSH server is classified into seven phases: connection establishment, version negotiation, key exchange and algorithm negotiation, user authentication, session request, session interaction, and session closure.

- Connection establishment
  - a The server listens on Transmission Control Protocol (TCP) port 22 and waits for a connection request from the client.
  - b The client initiates a TCP connection request to port 22 of the server to establish a TCP connection with the server.
- Version negotiation
  - a The server sends a version negotiation packet to the client.
  - b The client receives and processes the packet and replies the version to be used to the server.
  - c The server processes the reply from the client and determines whether version negotiation is successful.
- Key exchange and algorithm negotiation

  If the version negotiation succeeds, key exchange and algorithm negotiation are performed.
  - a The server and the client exchange the algorithm negotiation packet with each other and determine the final algorithm based on their capacity.

b The server and the client work together to generate a session key and session ID according to the key exchange algorithm and host key, which will be applied to subsequent user authentication, data encryption, and data decryption.

- User authentication

  After the encrypted channel is set up, user authentication is performed.

  a The client sends an authentication request to the server.

  b The server repeatedly conducts authentication for the client until the authentication succeeds or the server shuts down the connection because the maximum number of authentication attempts is reached.

- Session request

  a After the authentication is successful, the client sends a session request to the server.

  b The server waits and processes the client's session request. After the session request is successfully processed, the SSH client and server enter the session interaction phase.

- Session interaction

  In this phase, bidirectional transmission and processing of encrypted data are allowed.

  a The client sends commands that need to be executed to the server.

  b The server decrypts, parses, and processes these commands.

  c The server encrypts and sends the processing result to the client.

  d The client decrypts and processes the message from the server.

- Session closure

  The server and client disconnect the connection, and close the session.

3. User Authentication Mechanism

SSH supports password authentication, public key authentication, and other client authentication mechanisms.

- Password authentication

  Password authentication authenticates a client by verifying the username and password.

  a The client sends encrypted username and password to the server to request password authentication.

  b After receiving the request, the server decrypts the information, authenticates the client's identity through the Authentication, Authorization and Accounting (AAA) service (including local authentication and remote authentication), and sends an authentication success or failure message to the client.

- Public key authentication

  Public key authentication uses digital signature algorithms, such as Rivest-Shamir-Adleman (RSA) and Digital Signature Algorithm (DSA) to authenticate a client.

  a The client sends a public key authentication request to the server. This request contains information, including the username, public key, and public key algorithm.

  b After receiving the request, the server checks whether the public key is valid.

  c If not, the server directly returns an authentication failure message. If yes, the server performs digital signature authentication on the client and returns a message indicating successful or failed authentication.

Instruction

Public key authentication applies only to SSHv2 clients.

4. Public Key Algorithm

A public key algorithm is an asymmetric encryption algorithm used to encrypt communication data between an SSH client and server to ensure data transfer security.

The device supports three public key algorithms: RSA, DSA, and Elliptic Curves Cryptography (ECC).

- RSA

  RSA is based on most factorization algorithms and can be used for key and signature exchange. Due to low encryption and decryption efficiency, it does not apply to encryption and decryption of a large number of data.

- DSA

  Compared with RSA, DSA can be used only for signature and cannot be used for data encryption and decryption or key exchange. However, its efficiency is much higher than that of RSA.

- ECC

  ECC is based on the discrete logarithm algorithm and is difficult to be cracked down. In same security conditions, ECC has higher processing efficiency and lower storage and bandwidth requirements than RSA and DSA.

1.1.3 Protocols and Standards

- RFC 4251: The Secure Shell (SSH) Protocol Architecture
- RFC 4252: The Secure Shell (SSH) Authentication Protocol
- RFC 4253: The Secure Shell (SSH) Transport Layer Protocol
- RFC 4254: The Secure Shell (SSH) Connection Protocol
- RFC 4419: Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
- RFC 4716: The Secure Shell (SSH) Public Key File Format
- RFC 4819: Secure Shell Public Key Subsystem
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 1950: ZLIB Compressed Data Format Specification version 3.3

1.2 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

(1) Configuring SSH Server

- Enabling SSH Server
- (Optional) Configuring the SSH Server Version
- (Optional) Configuring the Listening Port
- (Optional) Configuring the Key and Key Exchange Algorithm of the SSH Server

- (Optional) Configuring the Encryption Algorithm
- (Optional) Configuring Authentication Parameters
- (Optional) Configuring an ACL
- (Optional) Configuring IP Address Blocking
- (Optional) Disconnecting an SSH Client Connection

(2) Configuring SCP Server

(3) Configuring SSH Client

- Establishing a Connection with the SSH Server
- (Optional) Restoring an Established SSH Client Session
- (Optional) Disconnecting a Suspended SSH Client Session

(4) Configuring SCP Client

1.3 Configuring SSH Server

1.3.1 Overview

After the SSH server function is configured on a device, SSH clients can remotely log in to the device.

1.3.2 Configuration Tasks

SSH server configuration includes the following tasks:

- Enabling SSH Server
- (Optional) Configuring the SSH Server Version
- (Optional) Configuring the Listening Port
- (Optional) Configuring the Key and Key Exchange Algorithm of the SSH Server
- (Optional) Configuring the Encryption Algorithm
- (Optional) Configuring Authentication Parameters
- (Optional) Configuring an ACL
- (Optional) Configuring IP Address Blocking
- (Optional) Disconnecting an SSH Client Connection

1.3.3 Enabling SSH Server

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the SSH server function.

enable service ssh-server

The SSH server function is disabled by default.

(4) (Optional) Enable the SSHv1 function.

ip ssh compatible-ssh1x enable

The SSHv1 function is disabled by default.

To use the SSHv1 version, enable the SSHv1 function first.

1.3.4 Configuring the SSH Server Version

1. Overview

The SSH server supports the SSHv1 and SSHv2 versions. Compared with SSHv1, SSHv2 has higher performance and security. During actual configuration, select a proper SSH server version based on the client version and security requirements.

2. Restrictions and Guidelines

The SSH server is compatible with SSHv1 and SSHv2 clients by default, that is, clients of both versions can connect to the SSH server. After an SSH server version is configured, only clients of the corresponding version can connect to the server.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the SSH server version.

ip ssh version *version-type*

The SSH server is compatible with the SSHv1 and SSHv2 clients by default.

1.3.5 Configuring the Listening Port

1. Overview

An SSH server uses port 22 to listen to client connections by default. The listening port can be changed through configuration.

Port 22 is a protocol-defined standard port and vulnerable to attacks from malicious users. If an attacker accesses this port frequently in a short time, problems such as bandwidth waste and performance deterioration may occur. As a result, other users cannot access the server (that is, the DoS attack). Changing the listening port can effectively prevent the problems.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the listening port of the SSH server.

ip ssh port *ssh-monitor-port*

The default listening port of the SSH server is port **22**.

1.3.6 Configuring the Key and Key Exchange Algorithm of the SSH Server

1. Overview

The key and key exchange algorithm of the SSH server are configured to establish a communication connection between the client and server.

2. Restrictions and Guidelines

SSHv1 uses an RSA key, and SSHv2 uses an RSA or a DSA key. If an RSA key is generated, both SSHv1 and SSHv2 can use the key. If a DSA key is generated, only SSHv2 can use the key.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Generate the public key of the SSH server.

crypto key generate { **dsa** | **ecc** | **rsa** }

No public key is generated on the SSH server by default.

If no key is generated on the SSH server, this parameter must be configured. To delete the public key of the SSH server, run the **crypto key zeroize** { **dsa** | **ecc** | **rsa** } command instead of the **no** form of this command.

(4) Configure the DH key exchange algorithms supported by the SSH server.

ip ssh key-exchange { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** | **ecdh_sha2_nistp256** | **ecdh_sha2_nistp384** | **ecdh_sha2_nistp521** }

Ruijie SSHv2 servers support diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, ecdh_sha2_nistp256, ecdh_sha2_nistp384, and ecdh_sha2_nistp521 for key exchange, and SSHv1 servers support none by default.

1.3.7 Configuring the Encryption Algorithm

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the encryption modes supported by the SSH server.

ip ssh cipher-mode { **cbc** | **ctr** | **gcm** | **others** } *

The encryption modes supported by the SSH server are **ctr** and **gcm** by default.

It is approved that **cbc** and **others** encryption algorithms can be decrypted in a limited period of time. Therefore, organizations or companies that have high security requirements can set the encryption modes supported by the SSH server to **ctr** and **gcm** to enhance the security level of the SSH server.

(4) Configure the message authentication algorithms supported by the SSH server.

ip ssh hmac-algorithm { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }

SSHv1 servers do not support any message authentication algorithms, and SSHv2 servers support the MD5, SHA1, SHA1-96, MD5-96, sha2-256, and sha2-512 message authentication algorithms by default.

1.3.8 Configuring Authentication Parameters

1. Overview

Parameters related to user authentication include the authentication timeout time, number of authentication attempts, and public key authentication.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the user authentication timeout time on the SSH server.

ip ssh time-out *timeout-time*

The default user authentication timeout time on the SSH server is **120** seconds.

If authentication still does not succeed when the user authentication timeout time expires, user authentication fails.

(4) Configure the number of authentication attempts allowed on the SSH server.

ip ssh authentication-retries *retry-times*

The default maximum number of authentication attempts allowed on the SSH server is **3**.

If the number of authentication attempts of a user by using the account and password exceeds the configured number of authentication attempts, user authentication fails.

(5) Associate with the public key file and username of a client.

ip ssh peer *username* **public-key** { **dsa** | **ecc** | **rsa** } *filename-path*

If a client needs to use public key authentication, the client's public key and username need to be associated with the device. Only SSHv2 supports public key authentication.

1.3.9 Configuring an ACL

1. Overview

An ACL can filter out users who meet specific rules. This prevents unauthorized users from accessing the device through SSH and causing security risks.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ACL on the SSH server.

(IPv4 address)

ip ssh access-class { *acl-name* | *acl-number* }

No IPv4 ACL is configured on the SSH server by default.

(IPv6 address)

ipv6 ssh access-class *acl-name*

No IPv6 ACL is configured on the SSH server by default.

1.3.10 Configuring IP Address Blocking

1. Overview

When the number of authentication failures for login through SSH reaches the configured limit in an authentication failure count period, the source IP address is blocked. That is, the SSH client that uses this source IP address is not allowed to log in to the device to prevent the device being attacked. The SSH client can log in to the device only after the IP address is awakened. This function is enabled by default and can be manually disabled.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IP address blocking on the SSH server.

ip ssh ip-block disable

The IP address blocking function of the SSH server is enabled by default.

Run the **no** form of this command to disable this feature.

(4) (Optional) Configure the number of authentication failures for blocking an IP address and the time period for counting authentication failures on the SSH server.

ip ssh ip-block failed-times *failed-times* **period** *period-time*

The allowed maximum number of authentication failures is **6**, and the time period for counting authentication failures is **5** minutes by default.

(5) (Optional) Configure the time period for awakening blocked IP addresses on the SSH server.

ip ssh ip-block reactive *reactive-interval*

Blocked IP addresses are awakened every **5** minutes by default.

After the time period for awakening blocked IP addresses is reached, SSH clients using these IP addresses can log in to the SSH server again.

(6) (Optional) Clear user information with blocked IP addresses and authentication failures.

clear ssh ip-block { **all** | *ipv4-address* | *ipv6-address* }

After the user information is cleared, corresponding clients can log in to the SSH server again.

1.3.11 Disconnecting an SSH Client Connection

(1) Enter the privileged EXEC mode.

enable

(2) Disconnect an established SSH client connection.

disconnect ssh { **vty** *session-id* | *session-id* }

Serving as an SSH server, the device may connect to multiple SSH clients. You can run this command to forcibly disconnect a client from the device. The client disconnection methods are as follows:

- Specify an SSH session ID. To display the SSH session ID of a client, run the **show ssh** command.
- Specify a Virtual Teletype (VTY) session ID. To display the VTY session ID of a client, run the **show users** command. This command can be used to disconnect SSH connections only.

1.4 Configuring SCP Server

1.4.1 Overview

Secure copy protocol (SCP) is a protocol that supports network file transfer. SCP is implemented based on RCP. RCP is responsible for file transfer, and SSH provides the authentication and encryption functions for RCP.

After the SCP server function is configured on the device, users can run the **scp** command to upload files to or download files from the device. Data exchanged during the process is encrypted for security.

1.4.2 Restrictions and Guidelines

The SSH server function must be enabled before the SCP server function is configured.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the SCP server function.

ip scp server enable

The SCP server function is disabled by default.

(4) (Optional) Configure the transmission path for uploading files to or downloading files from the SCP server.

ip scp server topdir { **flash:/***path* | **tmp:/***path* | **usb0:/***path* }

The default transmission path for file upload and download is **flash:/**.

1.5 Configuring SSH Client

1.5.1 Overview

When the local device is configured as an SSH client, the device can establish an SSH connection to another device that provides the SSH server service to remotely log in to the device for management operations.

1.5.2 Configuration Tasks

SSH client configuration includes the following tasks:

(1) Establishing a Connection with the SSH Server

(2) (Optional) Restoring an Established SSH Client Session

(3) (Optional) Disconnecting a Suspended SSH Client Session

1.5.3 Establishing a Connection with the SSH Server

(1) Enter the privileged EXEC mode.

enable

(2) Establish a remote encrypted session with the SSH server as an SSH client.

ssh [**oob**] [**-v** { **1** | **2** } | **-c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **-l** *username* | **-m** { **hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** | **hmac-sha2-256** | **hmac-sha2-512** } | **-p** *port-num*] * { *ip-address* | *hostname* } [**via** *mgmt-name*] [**/source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }] [**/vrf** *vrf-name*]

SSHv1 supports only the DES (56-bit key) and 3DES (168-bit key) encryption algorithms. SSHv2 supports the following Advanced Encryption Standards (AES): ASE128-CBC, AES192-CBC, AES256-CBC, AES128-CTR, AES192-CTR, and AES256-CTR. If you specify an unmatched encryption or authentication algorithm when selecting an SSH version, the unmatched algorithm will be ignored when a connection is established.

(3) Enter the global configuration mode.

configure terminal

(4) (Optional) Configure the source interface of the SSH client.

ip ssh source-interface *interface-type interface-number*

No SSH client source interface is configured by default.

After the source interface is configured, the SSH client uses the IP address on this interface as the global source address during communication. If no source interface is configured, the source address of SSH packets will be obtained by querying the corresponding route based on the destination address. If no source interface or source IP address is independently specified for an SSH connection, the global configuration is used.

1.5.4 Restoring an Established SSH Client Session

1. Overview

After the device establishes an SSH session with the SSH server as a client, you can press Ctrl+Shift+6+X to exit the session temporarily. After exiting the session, you can run the corresponding command to restore the session.

2. Restrictions and Guidelines

To display information about the SSH connections established by the device as an SSH client, run the **show ssh-session** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Restore an established SSH client session.

ssh-session *session-id*

1.5.5 Disconnecting a Suspended SSH Client Session

1. Overview

After the device connects to the SSH server as an SSH client, you can run the corresponding command to disconnect an SSH session with the specified session ID.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Disconnect a suspended SSH client session.

disconnect ssh-session *session-id*

You can run the **show ssh-session** command to display *session-id* of the device.

1.6 Configuring SCP Client

1.6.1 Overview

When the local device is configured as an SCP client, the device can run the **scp** command to upload files to or download files from a device that provides the SCP server service. Data exchanged during the process is encrypted for security.

1.6.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the source interface of the SCP client.

ip scp client source-interface *interface-type interface-number*

No SCP client source interface is configured by default.

After the source interface is configured, the SCP client uses the IP address on the interface as the global source address during communication. If no source interface is configured, the source address of SCP packets will be obtained by querying the corresponding route based on the destination address. If no source interface or source IP address is independently specified for an SCP connection, the global configuration is used.

(4) Upload files to or download files from the remote SCP server as an SCP client.

scp [**oob**] [**-v** { **1** | **2** } | **-c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-gcm** | **aes256-gcm** } | **-m** { **hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** | **hmac-sha2-256** | **hmac-sha2-512** } | **-p** *port-num*] * *source-file destination-file* [**via** *mgmt-name*] [**/source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }] [**/vrf** *vrf-name*]

1.7 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** commands to output debugging information.

Notice

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

Table 1-1 Monitoring

Command	Purpose
show ip ssh	Displays effective configurations of the SSH server.
show ssh	Displays information about established SSH connections.
show ssh ip-block { **all** | **list** }	Displays information about blocked IP addresses and authentication failures.
show crypto key mypubkey { **dsa** | **ecc** | **rsa** }	Displays partial public key information of the SSH server.
show ssh-session	Displays information about established SSH client sessions.
debug ssh	Debugs sessions of the SSH server.
debug ssh client	Debugs sessions of the SSH client.

1.8 Configuration Examples

1.8.1 Configuring Line Password Authentication for SSH Users

1. Requirements

After the SSH server function is enabled on a device, users can use the password configured in line configuration mode to log in to the device.

2. Topology

Figure 1-1 Configuring Line Password Authentication for SSH Clients

3. Notes

- Enable the SSH server function.
- Configure the line password.
- Enable password authentication in the line.

4. Procedure

(1) Enable the SSH server function.

```
Device> enable
Device# configure terminal
Device(config)# enable service ssh-server
```

(2) Set the line password to **password1**.

```
Device(config)# line vty 0 4
Device(config-line)# password password1
```

(3) Enable password authentication in the line.

```
Device(config-line)# login
```

5. Verification

- Use the client software to log in to the device through SSH. The password is **password1**, and the username can be any value. Verify that the login is successful. Use the PuTTY software as an example. The login page is as follows:

```
login as: anyname
anyname@192.168.1.1's password:



Last login: Apr  2 2021 10:00:00 from 192.168.1.2 through ssh.
Device#
```

- Run the **show ip ssh** command to verify that the SSH server takes effect.

```
Device# show ip ssh
SSH Enable - version 2.0
SSH Port:             22
SSH Cipher Mode:       ctr,gcm
SSH HMAC Algorithm:    sha2-256,sha2-512
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server:        disabled
SSH ip-block:          enabled
```

- Run the **show ssh** command to display the SSH connection information. Verify that a connection with username **anyname** (used during login) exists.

```
Device# show ssh
Connection Version Encryption      Hmac        Compress   State
Username
        1    2.0 aes256-ctr      hmac-sha2-256 none      Session started
anyname
```

- Run the **show users** command to display information about connected clients.

```
Device#show users
Line           User        Host(s)            Idle      Location
---------------- ------------ -------------------- ---------- ----------------
--
```

```
  0 con 0      ---        idle              00:00:16   ---
* 1 vty 0      ---        idle              00:00:00   192.168.1.2
```

6. Configuration Files

```
!
enable service ssh-server
!
line console 0
line vty 0 4
 login
 password 7 $10$396$mnO2p3SVaxm7$
!
```

1.8.2 Configuring Local User Authentication for SSH Clients

1. Requirements

After the SSH server function is enabled on a device, users can use the local account created on the device to log in to the device through SSH.

2. Topology

Figure 1-2 Configuring Local User Authentication for SSH Clients

3. Notes

- Enable the SSH server function.
- Add a local user account.
- Enable local user authentication in the line.

4. Procedure

(1) Enable the SSH server function.

```
Device> enable
Device# configure terminal
Device(config)# enable service ssh-server
```

(2) Add a local user whose username is **hostname1** and password is **password1**.

```
Device(config)# username hostname1 password password1
```

(3) Enable local user authentication in the line.

```
Device(config)# line vty 0 4
Device(config-line)# login local
```

5. Verification

- Use the client software to log in to the device through SSH. The username is **hostname1**, and the password

is **password1**. Verify that the login is successful. Use the PuTTY software as an example. The login page is as follows:

```
login as: hostname1
hostname1@192.168.1.1's password:



Last login: Apr  2 2021 10:00:00 from 192.168.1.2 through ssh.
Device>
```

- Run the **show ip ssh** command to verify that the SSH server takes effect.

```
Device# show ip ssh
SSH Enable - version 2.0
SSH Port:             22
SSH Cipher Mode:       ctr,gcm
SSH HMAC Algorithm:    sha2-256,sha2-512
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server:        disabled
SSH ip-block:          enabled
```

- Run the **show ssh** command to display the SSH connection information. Verify that a connection with username **hostname1** exists.

```
Device# show ssh
Connection Version Encryption      Hmac        Compress   State
Username
        1    2.0 aes256-ctr      hmac-sha2-256 none      Session started
hostname1
```

- Run the **show users** command to display information about connected clients. Verify that a client whose username is **hostname1** exists.

```
Device#show users
Line           User        Host(s)            Idle      Location
---------------- ------------ -------------------- ---------- ----------------
--
   0 con 0      ---         idle               00:00:16   ---
*  1 vty 0      hostname1    idle               00:00:00   192.168.1.2
```

6. Configuration Files

```
!
username hostname1 password 7 $10$2fe$Rd/C4ijEl+UN$
!
enable service ssh-server
!
line console 0
line vty 0 4
 login local
!
```

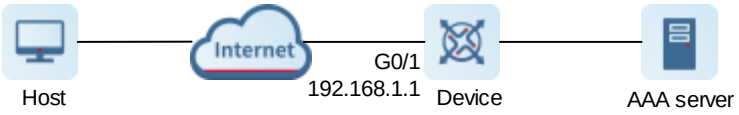
1.8.3 Configuring AAA Authentication for SSH Clients

1. Requirements

SSH clients can be authenticated using the AAA mode.

2. Topology

Figure 1-3 Configuring AAA Authentication for SSH Clients



3. Notes

- Configure the AAA server and add an AAA user on the AAA server.
- Enable the SSH server function.
- Enable the AAA service on the device and set the SSH authentication method to AAA server.
- Enable AAA authentication in the line.

4. Procedure

(1) Configure the AAA server and add an AAA user whose username is **hostname1** and password is **password1** on the AAA server. (For details about AAA server configuration, see the AAA server configuration guide.)

(2) Enable the SSH server function.

```
Device> enable
Device# configure terminal
Device(config)# enable service ssh-server
```

(3) Enable AAA services.

```
Device(config)# aaa new-model
```

(4) Configure the address and shared key of the AAA server (a RADIUS server is used as an example here, the IP address is set to **192.168.1.3**, and the shared key is set to **radiuskey**).

```
Device(config)# radius-server host 192.168.1.3 key radiuskey
```

(5) Configure the login authentication method list **login-method** and select **radius** as the authentication method. The backup method **local** is configured. This ensures that a backup solution is available when the AAA server is faulty.

```
Device(config)# aaa authentication login login-method group radius local
```

(6) Enable AAA authentication in the line.

```
Device(config)# line vty 0 4
Device(config-line)# login authentication login-method
```

5. Verification

- Use the client software to log in to the device through SSH. The username is **hostname1**, and the password is **password1**. Verify that the login is successful. Use the PuTTY software as an example. The login page is as follows:

```
login as: hostname1
hostname1@192.168.1.1's password:



Last login: Apr  2 2021 10:00:00 from 192.168.1.2 through ssh.
Device>
```

- Run the **show ip ssh** command to verify that the SSH server takes effect.

```
Device# show ip ssh
SSH Enable - version 2.0
SSH Port:             22
SSH Cipher Mode:       ctr,gcm
SSH HMAC Algorithm:    sha2-256,sha2-512
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server:        disabled
SSH ip-block:         enabled
```

- Run the **show ssh** command to display the SSH connection information. Verify that a connection with username **hostname1** exists.

```
Device# show ssh
Connection Version Encryption      Hmac        Compress   State
Username
        1    2.0 aes256-ctr      hmac-sha2-256 none      Session started
hostname1
```

- Run the **show users** command to display information about connected clients. Verify that a client whose username is **hostname1** exists.

```
Device#show users
Line           User        Host(s)            Idle      Location
---------------- ------------ -------------------- ---------- ----------------
--
   0 con 0      ---         idle               00:00:16   ---
*  1 vty 0      hostname1    idle               00:00:00   192.168.1.2
```

6. Configuration Files

```
!
aaa new-model
aaa authentication login login-method group radius local
!
radius-server host 192.168.1.3 key 7 $10$3b4$ln0s66i8XfEi$
!
line vty 0 4
 login authentication login-method
!
```

1.8.4 Configuring Public Key Authentication for SSH Clients

1. Requirements

When the device serves as the SSH server, users can use public key authentication to log in to the device without needing a password.

2. Topology

Figure 1-4 Configuring Public Key Authentication for SSH Clients

3. Notes

- Use the client software to generate a pair of keys (public key and private key).
- Copy the public key file to the flash memory of the device and associate the key with the user.

4. Procedure

(1) Configure a local user and enable local user authentication in a line. For details, see 1.8.2 Configuring Local User Authentication for SSH Clients.

(2) Use the client software to generate a pair of keys. The Ubuntu environment is used as an example. The generated private key is **id_rsa** and public key is **id_rsa.pub**.

```
root@ubuntu:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:6a/sWJjpx97QQEs9Aoiph5Ry452ybIyNyZUsT48Irrw root@ubuntu
The key's randomart image is:
+---[RSA 2048]----+
|  .o ..          |
|.o= .  . .       |
|o=.o..  + o      |
|+.+=o  o + .     |
|+O*oo   S        |
|++*o . = o       |
|o.    +.+ .      |
|..   . +o+       |
| E.   o+=.o      |
+----[SHA256]-----+
```

(3) Copy the public key file to the flash memory of the device (omitted).

(4) Associate the public key with **hostname1**.

```
Device> enable
Device# configure terminal
Device(config)# ip ssh peer hostname1 public-key rsa flash:test_key.pub
```

5. Verification

Verify that users can log in to the device through public key authentication. (The Ubuntu environment is used as an example.)

```
root@ubuntu:~/.ssh# ls
id_rsa  id_rsa.pub
root@ubuntu:~/.ssh# ssh -i id_rsa hostname1@192.168.1.1



Last login: Apr 2 2021 10:00:00 through console.
Device>
```

6. Configuration Files

```
!
username hostname1 password 7 $10$2fe$Rd/C4ijEl+UN$
!
ip ssh peer hostname1 public-key rsa flash:id_rsa.pub
!
enable service ssh-server
!
line console 0
line vty 0 4
 login local
!
```

1.8.5 Configuring SCP Server

1. Requirements

When the device serves as the SCP server, users can run the **scp** command to upload files to and download files from the device.

2. Topology

Figure 1-5 Configuring SCP Server

3. Notes

- Enable the SSH server function.
- Enable the SCP server function.

4. Procedure

(1) Configure a local user and enable local user authentication in a line. For details, see 1.8.2 Configuring Local User Authentication for SSH Clients.

(2) Enable the SSH server function.

```
Device> enable
Device# configure terminal
Device(config)# enable service ssh-server
```

(3) Enable the SCP server function.

```
Device(config)# ip scp server enable
```

5. Verification

Verify that the client can run the **scp** command to upload files to the device. The Ubuntu environment is used as an example here.

(1) In the Ubuntu shell environment, run the **scp** command to upload **file.txt** to the device.

```
root@ubuntu:~# scp file.txt hostname1@192.168.1.1:/
hostname1@192.168.1.1's password:
file.txt                                  100%   14     0.0KB/s   00:00
```

(2) Check whether **file.txt** exists in the flash directory of the device.

```
Device> enable
Device# dir flash:file.txt
Number  Properties     Size            Time                   Name
------  ----------  ----------  ------------------------  --------------------
  1       -rwx      14B       Fri Apr 2 10:00:00 2021  file.txt
```

Verify that the client can run the **scp** command to download files from the device. The Ubuntu environment is used as an example here.

(1) The **file.txt** file exists in the flash directory of the device.

```
Device> enable
Device# dir flash:file.txt
Number  Properties     Size            Time                   Name
------  ----------  ----------  ------------------------  --------------------
  1       -rwx      14B       Fri Apr 2 10:00:00 2021  file.txt
```

(3) In the Ubuntu shell environment, run the **scp** command to download **file.txt** from the device and rename it as **file1.txt**.

```
root@ubuntu:~# scp hostname1@192.168.1.1:/file.txt file1.txt
hostname1@192.168.1.1's password:
file.txt                                  100%   14     0.0KB/s   00:00
```

(4) In the Ubuntu shell environment, verify that the **file1.txt** file has been downloaded.

```
root@ubuntu:~# ls -l file1.txt
-rwxr--r-- 1 root root 14 Apr 2 10:00 file1.txt
```

6. Configuration Files

```
!
```

```
username hostname1 password 7 $10$2fe$Rd/C4ijEl+UN$
!
enable service ssh-server
!
ip scp server enable
!
line console 0
line vty 0 4
 login local
!
```

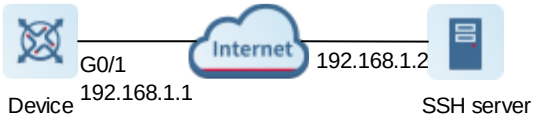
1.8.6 Configuring SSH Client

1. Requirements

When the device serves as an SSH client, the device can log in to the SSH server through SSH.

2. Topology

Figure 1-6 Configuring SSH Client



3. Notes

- Configure a valid user on the SSH server.
- Run the **ssh** command to log in to the SSH server.

4. Procedure

(1) Configure a valid user on the SSH server. (For details, see the SSH server user manual.)

(2) Run the **ssh** command to log in to the SSH server.

```
Device> enable
Device# ssh -l admin 192.168.1.2
```

5. Verification

Verify that the device logs in to the SSH server successfully.

```
Device# ssh -l hostname1 192.168.1.2
%Trying 192.168.1.2, 22,...open
hostname1@192.168.1.2's password:



Last login: Apr 2 2021 10:00:00 from 192.168.1.1 through ssh.
```

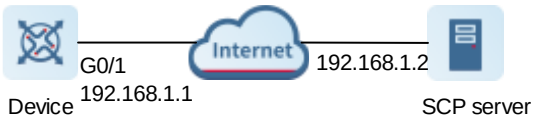
1.8.7 Configuring SCP Client

1. Requirements

When the device serves as an SCP client, the device can run the **scp** command to upload files to and download files from the SCP server.

2. Topology

Figure 1-7 Configuring SCP Client



3. Notes

- Configure a valid user on the SCP server.
- Run the **scp** command to upload files to or download files from the SCP server.

4. Procedure

(1) Configure a valid user on the SCP server. For details, see the SCP server user manual.

(2) Run the **scp** command to copy **file.txt** from the SCP server to the flash memory of the device.

```
Device> enable
Device# scp hostname1@192.168.1.2:/file.txt flash:/file.txt
```

(3) Run the **scp** command to copy local file **file.txt** from the device to the SCP server.

```
Device> enable
Device# scp hostname1@192.168.1.2:/file.txt flash:/file.txt
```

5. Verification

- Verify that the file on the SCP server is successfully copied to a local directory.

```
Device> enable
Device# scp oob flash:/file.txt hostname1@192.168.1.2:/file.txt

%Trying 192.168.1.2, 22,...open
hostname1@192.168.1.2's password:
Press Ctrl+C to quit
!
Transmission success.
```

- Verify that the local file is successfully copied to the SCP server.

```
Device> enable
Device# scp hostname1@192.168.1.2:/file.txt flash:/file.txt

%Trying 192.168.1.2,...open
hostname1@192.168.1.2's password:
Press Ctrl+C to quit
!
```

```
Transmission success.
```

Contents

1 Configuring Global IP-MAC Address Binding 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Restrictions and Guidelines 2

1.3 Configuring Global IP-MAC Address Binding 2

1.4 Monitoring 3

1 Configuring Global IP-MAC Address Binding

1.1 Introduction

1.1.1 Overview

The global IP-Media Access Control (MAC) address binding function is used to verify the IP address and MAC address binding relationship of input packets. If a specified IP address is bound with a MAC address, the device receives only the IP packets containing matched IP address and MAC address. The other packets are discarded.

The address binding function strictly controls the validity of input packets to improve network security.

The address binding function has higher priority than 802.1x authentication, port security, and access control list (ACL) in controlling the validity of input packets.

1.1.2 Principles

1. IPv6 Address Binding Mode

IPv6 address binding modes include the compatible, loose, and strict modes. The default mode is the strict mode. If the IPv4-MAC address binding policy is not configured, the IPv6 packet forwarding control rules based on the IPv4-MAC address binding policy do not take effect and all IPv4 and IPv6 packets are allowed to pass through. If the IPv4-MAC address binding policy is configured, the IPv6 packet forwarding control rules take effect, and the device forwards IPv4 and IPv6 packets based on the forwarding rules. The following table describes the forwarding rules.

Table 1-1 Forwarding Rules

Binding Mode	IPv4 Packet Forwarding Rule	IPv6 Packet Forwarding Rule
Strict	Packets matching the IPv4-MAC address binding conditions are forwarded.	Packets matching the IPv6-MAC address binding conditions are forwarded.
Loose	Packets matching the IPv4-MAC address binding conditions are forwarded.	● If IPv6-MAC address binding is configured, packets matching the IPv6-MAC address binding conditions are forwarded. ● If IPv6-MAC address binding is not configured, all IPv6 packets are forwarded.
Compatible	Packets matching the IPv4-MAC address binding conditions are forwarded.	● IPv6 packets are forwarded if they contain MAC addresses matching the MAC address in the IPv4-MAC address binding policy. ● Packets matching the IPv6-MAC address binding conditions are forwarded.

The IPv4-MAC address binding policy can be generated by global IP-MAC address binding or other access security functions, such as port security and IP source guard.

The IPv6-MAC address binding policy can be generated by global IPv6-MAC address binding or other access security functions, such as port security and IPv6 source guard.

2. Excluded Ports

The IP-MAC address binding function takes effect on all ports of the device by default. You can configure excluded ports on which this function does not take effect. In practice, the IP-MAC address bindings of the IP packets on the uplink port are not fixed. Generally, the uplink port of the device is configured as an excluded port so that the packets on the uplink port are not checked for IP-MAC address binding.

1.2 Restrictions and Guidelines

- When no IP-MAC address binding policy is configured, the IP-MAC address binding function does not take effect after the **address-bind install** command is run and all packets are allowed to pass through.
- The **address-bind uplink** *interface-type interface-number* command can configure only switching ports or layer 2 (L2) aggregation ports (APs) as excluded ports for address binding.

1.3 Configuring Global IP-MAC Address Binding

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a global IP-MAC address binding policy.

address-bind { *ipv4-address mac-address* | *ipv6-address mac-address* }

No IP-MAC address binding policy is configured by default.

(4) (Optional) Configure a port as an excluded port for address binding.

address-bind uplink *interface-type interface-number*

No port is configured as an excluded port for address binding by default.

(5) Enable the IP-MAC address binding function.

address-bind install

The IP-MAC address binding function is disabled by default.

(6) (Optional) Configure the IPv6 address binding mode.

address-bind ipv6-mode { **compatible** | **loose** | **strict** }

The default IPv6 address binding mode is the strict mode.

(7) (Optional) Enable address binding log filtering.

address-bind binding-filter logging [**rate-limit** *rate*]

Address binding log filtering is disabled by default.

1.4 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-2 Monitoring

Command	Purpose
show address-bind	Displays the global IP-MAC address binding policy.
show address-bind uplink	Displays excluded ports for address binding.

Contents

1 Configuring Port Security 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Restrictions and Guidelines 2
1.3 Configuration Task Summary 2
1.4 Configuring Secure Ports 2
1.4.1 Overview 2
1.4.2 Restrictions and Guidelines 2
1.4.3 Procedure 2
1.5 Configuring Secure Address Management 3
1.5.1 Overview 3
1.5.2 Procedure 4
1.6 Configuring Static Secure Addresses 4
1.6.1 Overview 4
1.6.2 Restrictions and Guidelines 4
1.6.3 Procedure 4
1.7 Configuring Secure Address Binding 5
1.7.1 Overview 5
1.7.2 Restrictions and Guidelines 5
1.7.3 Procedure 5
1.8 Enabling Binding Log Filtering 6
1.8.1 Overview 6

1.8.2 Procedure.....6

1.9 Monitoring 6

1.10 Common Errors.....6

1 Configuring Port Security

1.1 Introduction

1.1.1 Overview

Port security is used to control packets entering a device port based on the source Media Access Control (MAC) address in the packets.

You can configure static MAC addresses or the maximum number of dynamically learned MAC addresses on a port to control packets entering the port.

Ports configured with port security are called secure ports.

1.1.2 Principles

1. Basic Concepts

- Secure port

  Ports configured with port security are called secure ports.

- Secure address and maximum number of secure addresses

  Addresses bound to secure ports are called secure addresses. Secure addresses can be layer 2 (L2) addresses, namely, MAC addresses, or layer 3 (L3) addresses, namely, IP addresses or IP addresses and MAC addresses.

  The maximum number of secure addresses is the sum of statically configured secure addresses and dynamically learned secure addresses. When the number of secure addresses for a secure port does not reach the maximum number, the secure port can dynamically learn new secure addresses. When the number of secure addresses for the secure port reaches the maximum number, the secure port will not learn dynamic secure addresses any longer. If a new user host accesses the secure port after the number of secure addresses reaches the maximum number, a security violation event occurs.

- Dynamic binding

  The device automatically learns addresses and converts learned addresses into secure addresses.

- Static binding

  You can manually configure secure addresses.

2. Port Security and Security Violation

After port security is enabled on a port, user packets that access the network through the port will be controlled.

The security module of the device will check the source MAC addresses of received packets. Only packets from addresses in the secure address list will be forwarded, and other packets will be discarded.

When the number of MAC addresses learned by a port exceeds the maximum number of secure addresses, a security violation event is triggered. You can configure the following modes for handling security violation events:

- **protect**: When security violation occurs, the corresponding secure port stops learning MAC addresses and discards all packets of newly accessed users. This is the default violation handling mode.
- **restrict**: When security violation occurs, a port violation trap notification will be sent in addition to the behavior

in **protect** mode.

- **shutdown**: When security violation occurs, the port will be disabled in addition to the behavior in **protect** mode.

If the number of user hosts connected to a port is less than the maximum number of secure addresses after a security violation event occurs, the port is restored to the non-violation state.

1.2 Restrictions and Guidelines

When port security is configured together with other access control functions, such as 802.1x and IP source guard, packets can enter a port only after the packets pass through all security check rules. If a security channel or global IP-MAC address binding is configured on a port, packets that meet the security channel or global IP-MAC address binding conditions will be exempted from port security check.

1.3 Configuration Task Summary

Port security configuration includes the following tasks:

(1) Configuring Secure Ports

(2) (Optional) Configuring Secure Address Management

(3) (Optional) Configuring Static Secure Addresses

(4) (Optional) Configuring Secure Address Binding

(5) (Optional) Enabling Binding Log Filtering

1.4 Configuring Secure Ports

1.4.1 Overview

After port security is enabled on a port, you can configure the method for handling packets that violate port security requirements.

1.4.2 Restrictions and Guidelines

- The port security function can be configured only on switching ports and L2 aggregation ports (APs).
- Switch Port Analyzer (SPAN) destination ports cannot be configured as secure ports.
- The port security function cannot be configured for Dynamic Host Configuration Protocol (DHCP) Snooping trusted ports.
- The port security function cannot be configured for excluded ports of global IP-MAC address binding.
- **protect** indicates that the device discards packets that do not match the security address. **restrict** indicates that the device discards packets that do not match the security address and sends a trap notification. **shutdown** indicates that the device discards packets that do not match the security address and disables the port.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable port security.

switchport port-security

The port security function is disabled by default.

(5) (Optional) Configure the method for handling packets that violate port security requirements.

switchport port-security violation { **protect** | **restrict** | **shutdown** }

Packets that do not match the security address are discarded by default.

1.5 Configuring Secure Address Management

1.5.1 Overview

1. Maximum Number of Secure Addresses

The number of secure addresses is the sum of statically configured secure addresses and dynamically learned secure addresses. When the number of MAC addresses learned by a port exceeds the maximum number of secure addresses, a security violation event is triggered.

If you set the maximum number of secure addresses for a port to **1** and configure a secure address for this port, the workstation (whose address is the configured secure address) connected to this port will exclusively use all bandwidth of the port.

The maximum number of secure addresses takes effect only to secure addresses and is invalid to security bindings.

By configuring the maximum number of secure addresses and secure address aging time, the device can automatically add and delete secure addresses on a port.

2. Secure Address Aging

After the secure address aging time is configured, an aging timer is triggered to regularly query and delete secure addresses whose aging time expires. By configuring the maximum number of secure addresses and secure address aging time, the device can automatically add and delete secure addresses on a port.

The **switchport port-security aging time** *aging-time* command is used to configure the secure address aging time, in minutes. The value range is from 0 to 1440. The default secure address aging time is **0**, which indicates that secure addresses never age. If a non-zero value is configured, the device regularly queries and deletes secure addresses based on the configured time. When a non-zero aging time is configured, only dynamically learned addresses are aged by default. If the **switchport port-security aging static** command is configured, statically configured and dynamically learned secure addresses are aged.

3. Sticky MAC Address

Sticky MAC addresses are special MAC addresses not affected by the aging mechanism. No matter whether dynamic or static aging is configured, sticky MAC addresses will not be aged.

If dynamically learned secure addresses are saved as static sticky MAC addresses, these addresses will not age. After the configurations are saved, these addresses do not need to be learned again upon a restart. If this function is not enabled, these addresses must be learned again after a device restart.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum number of secure addresses for a port.

switchport port-security maximum *number*

The default maximum number of secure addresses for a port is **128**.

(5) Configure the secure address aging time and its application scope on a port.

switchport port-security aging { **static** | **time** *aging-time* }

The secure address aging time is **0** (that is, not aged), and the aging time applies only to dynamically learned addresses by default.

(6) Enable sticky MAC address learning and configure sticky MAC addresses.

switchport port-security mac-address sticky [*mac-address* [**vlan** *vlan-id*]]

Sticky MAC address learning is disabled by default.

1.6 Configuring Static Secure Addresses

1.6.1 Overview

After static secure addresses are configured on a secure port, only specified users can use this port. The secure addresses are periodically updated to ensure network security.

1.6.2 Restrictions and Guidelines

- The maximum number of secure addresses configured by running the **switchport port-security maximum** *number* command takes effect only to secure addresses, and the number of security bindings is not limited.
- If security binding and a static secure MAC address are configured, the static secure MAC address must be the same as the MAC address in the IP-MAC address binding. Otherwise, communication may fail due to inconsistency with the binding. Similarly, if only IP address binding is configured, only packets whose secure MAC addresses are statically configured or dynamically learned and whose source IP address is the bound IP address can enter the device.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure static secure addresses for a port. Please configure only one task.

- Configure static secure addresses for a port in global configuration mode.

  switchport port-security interface *interface-type interface-number* **mac-address** *mac-address* [**vlan** *vlan-id*]

  No static secure address is configured for a port by default.

- Enter the interface configuration mode of the port and configure static secure addresses.

  interface *interface-type interface-number*

  switchport port-security mac-address *mac-address* [**vlan** *vlan-id*]

  No static secure address is configured for a port by default.

1.7 Configuring Secure Address Binding

1.7.1 Overview

When security binding (IP address binding or IP-MAC address binding) is configured, IP packets are first checked for secure addresses (including statically configured and dynamically learned secure addresses). If secure address check fails, the IP packets are discarded. If secure address check is successful, the bound IP address is checked. If IP address check is successful, the data packets are forwarded. Otherwise, the packets are discarded.

1.7.2 Restrictions and Guidelines

- The maximum number of secure addresses configured by running the **switchport port-security maximum** *number* command takes effect only to secure addresses, and the number of security bindings is not limited.
- If security binding and a static secure MAC address are configured, the static secure MAC address must be the same as the MAC address in IP-MAC address binding. Otherwise, communication may fail due to inconsistency with the binding. Similarly, if only IP address binding is configured, only packets whose secure MAC addresses are statically configured or dynamically learned and whose source IP address is the bound IP address can enter the device.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure security bindings. Please configure only one task.

- Configure security bindings for a port in global configuration mode.

  switchport port-security interface *interface-type interface-number* **binding** [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

  No security binding is configured by default.

- Enter the interface configuration mode of the port to be bound and configure security binding.

  interface *interface-type interface-number*

  switchport port-security binding [*mac-address* **vlan** *vlan-id*] { *ipv4-address* | *ipv6-address* }

  No secure address is bound to a port by default.

1.8 Enabling Binding Log Filtering

1.8.1 Overview

After the binding log filtering function is enabled, the device prints alert logs if received IP packets do not match the bound IP and MAC addresses or the bound IP address for port security.

When the binding log printing rate exceeds the configured rate, the number of suppressed logs will be displayed.

1.8.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Enable binding log filtering.

switchport port-security binding-filter logging [**rate-limit** *rate*]

Address binding log filtering is disabled by default.

1.9 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show port-security	Displays all port security configurations.
show port-security all	Displays all effective secure addresses and secure address bindings on a port.
show port-security address [**interface** *interface-type interface-number*]	Displays secure addresses of all ports or a specified port.
show port-security binding [**interface** *interface-type interface-number*]	Displays secure address bindings of all ports or a specified port.
show port-security interface *interface-type interface-number*	Displays port security configurations of a specified port.

1.10 Common Errors

- Port security is enabled on a SPAN port.

- Port security is enabled on a DHCP trusted port.
- The configured maximum number of secure addresses is smaller than the current number of secure addresses.

Contents

1 Configuring IP Source Guard 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Restrictions and Guidelines 2
1.3 Configuration Task Summary 2
1.4 Enabling IP Source Guard on an Interface 2
1.4.1 Restrictions and Guidelines 2
1.4.2 Prerequisites 2
1.4.3 Procedure 2
1.5 Enabling IP Source Guard on a VLAN 3
1.5.1 Overview 3
1.5.2 Prerequisites 3
1.5.3 Procedure 3
1.6 Enabling the Sole Role of the IP Source Address Binding Database as the Source of DAI Binding Entries 4
1.6.1 Overview 4
1.6.2 Procedure (Interface Configuration Mode) 4
1.6.3 Procedure (VLAN Configuration Mode) 4
1.7 Monitoring 5
1.8 Common Errors 5

1 Configuring IP Source Guard

1.1 Introduction

1.1.1 Overview

The IP Source Guard function enables the hardware to filter IP packets to ensure that only users whose IP packets match information in the database of the hardware can access the network normally, preventing users from privately setting IP addresses or forging IP packets.

1.1.2 Principles

1. Basic Concepts

- Source IP address

  Indicate the source IP address field in IP packets.

- Source MAC address

  Indicate the source media access control (MAC) address field in L2 packets.

- User record binding database

  The user record binding database is the basis for IP Source Guard. Data in the user record binding database comes from the following two sources:

  Dynamic Host Configuration Protocol (DHCP) Snooping binding database: When IP Source Guard is enabled, data of the DHCP Snooping binding database is synchronized to the user record binding database of IP Source Guard. In this case, IP packets are filtered strictly through IP Source Guard on devices with DHCP Snooping enabled.

  Static user configuration: static user information configured by running the **ip source binding** command.

- Excluded VLAN

  When IP Source Guard is enabled on an interface, it is effective to all the virtual local area networks (VLANs) under the interface by default. Users can specify excluded VLANs, within which IP packets are not checked or filtered, that is, such IP packets are not controlled by IP Source Guard. A maximum of 32 excluded VLANs can be specified for one interface.

2. Checking the Source Address Fields of Packets

IP packets passing through an interface are checked based on the source IP address or source IP address and MAC address to prevent malicious users from forging packets to launch attacks. When there is no need to check or filter IP packets within a VLAN, users can specify this VLAN as an excluded VLAN to release such packets.

When IP Source Guard is enabled on an interface, the device checks the source addresses of packets passing through the interface, which can be a switching interface, L2 aggregation port (link aggregation), or L2 encapsulation subinterface. Only the packets whose source addresses match entries in the user record binding database can pass through the interface. There are two matching methods:

- Filtering based on the source IP address

The source IP addresses of all IP packets passing through an interface are checked. Packets are allowed to pass through the interface only when the source IP addresses of these packets belong to the IP address set of the user record binding database. It is the default filtering policy of IP Source Guard.

- Filtering based on the source IP address and MAC address

  The source IP addresses and MAC addresses of IP packets passing through an interface are checked. Packets are allowed to pass through the interface only when both the L2 source MAC addresses and L3 source IP addresses of these packets match an entry in the user record binding database.

1.2 Restrictions and Guidelines

- Typically, IP Source Guard needs to work with DHCP Snooping. Therefore, DHCP Snooping should also be enabled. DHCP Snooping can be enabled either before or after IP Source Guard is enabled.
- IP Source Guard cannot be configured on the trusted interfaces of DHCP Snooping or IP Source Guard.
- IP Source Guard cannot be configured on the ports that do not verify the global IP address and MAC address binding.
- IP Source Guard can be configured based on interfaces or VLANs.

1.3 Configuration Task Summary

Select any of the following configuration tasks to configure.

- Enabling IP Source Guard on an Interface
- Enabling IP Source Guard on a VLAN
- Enabling the Sole Role of the IP Source Address Binding Database as the Source of DAI Binding Entries

1.4 Enabling IP Source Guard on an Interface

1.4.1 Restrictions and Guidelines

IP Source Guard can be enabled only on switching interfaces, L2 aggregation ports, or L2 encapsulation subinterfaces.

1.4.2 Prerequisites

DHCP Snooping is enabled by running the **ip dhcp snooping** command.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Add static user information to the source IP address binding database.

ip source binding *mac-address* **vlan** *vlan-id ipv4-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

No static user information is added by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) (Optional) Configure the function of converting source IP address binding entries to static MAC address entries.

ip source binding sticky-mac

The function of converting source IP address binding entries to static MAC address entries is disabled by default.

(6) Enable IP Source Guard on an interface.

ip verify source [**port-security**]

IP Source Guard is disabled on an interface by default.

(7) (Optional) Specify an excluded VLAN for IP Source Guard on an interface.

ip verify source exclude-vlan *vlan-id*

The function of specifying excluded VLANs for IP Source Guard on an interface is disabled by default.

Excluded VLANs can be specified on an interface only after IP Source Guard is enabled on the interface. Specified excluded VLANs will be deleted automatically when IP Source Guard is disabled on the interface.

1.5 Enabling IP Source Guard on a VLAN

1.5.1 Overview

When IP Source Guard is enabled on a VLAN, the source IP addresses of IP packets in the VLAN will be checked to filter out invalid IP packets.

1.5.2 Prerequisites

DHCP Snooping is enabled by running the **ip dhcp snooping** command.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Add static user information to the source IP address binding database.

ip source binding *mac-address* **vlan** *vlan-id ip-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

No static user information is added by default.

(4) Enter the VLAN configuration mode.

vlan { *vlan-id* | **range** *vlan-range* }

(5) Enable IPv6 Source Guard on a VLAN.

ipv6 **verify source** [**port-security**]

IP Source Guard is disabled on a VLAN by default.

(6) Return to the global configuration mode.

exit

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) (Optional) Configure trusted interfaces of IP Source Guard.

ip verify source trust

No IP Source Guard trusted interface is configured by default.

The IP Source Guard trusted interface function is mutually exclusive with the IP Source Guard interface, port security, 802.1x authorization, and Address Resolution Protocol (ARP) check services.

1.6 Enabling the Sole Role of the IP Source Address Binding Database as the Source of DAI Binding Entries

1.6.1 Overview

After the sole role of the source IP address binding database as the source of DAI binding entries is configured, the bound entries are solely used for Dynamic ARP Inspection (DAI) and are not assigned to the hardware. That is, IP Source Guard is not performed.

1.6.2 Procedure (Interface Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Add static user information to the source IP address binding database.

ip source binding *mac-address* **vlan** *vlan-id ip-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

No static user information is added by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Enable the sole role of the source IP address binding database as the source of DAI binding entries.

ip verify source dai-source

The sole role of the source IP address binding database as the source of DAI binding entries is not configured by default.

1.6.3 Procedure (VLAN Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Add static user information to the source IP address binding database.

ip source binding *mac-address* **vlan** *vlan-id ip-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

No static user information is added by default.

(4) Enter the VLAN configuration mode.

vlan { *vlan-id* | **range** *vlan-range* }

(5) Enable the sole role of the source IP address binding database as the source of DAI binding entries.

ip verify source dai-source

The sole role of the source IP address binding database as the source of DAI binding entries is not configured by default.

1.7 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show ip verify source [**interface** *interface-type interface-number* | **vlan** *vlan-id*]	Displays user filtering entries of IP Source Guard.
show ip source binding [*ipv4-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**dhcp-snooping** | **static**] [**inner-vlan** *inner-vid*]	Displays information of the source IP address binding database.
show ip source binding sticky-mac [**interface** *interface-type interface-number*]	Displays information about source IP address binding entries converted to static MAC address entries.

1.8 Common Errors

- IP Source Guard is enabled on a DHCP Snooping trusted interface.
- An excluded VLAN is specified before IP Source Guard is enabled.

Contents

1 Configuring IPv6 Source Guard 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Restrictions and Guidelines 2
1.3 Configuration Task Summary 2
1.4 Enabling IPv6 Source Guard on an Interface 2
1.4.1 Restrictions and Guidelines 2
1.4.2 Prerequisites 2
1.4.3 Procedure 2
1.5 Enabling IPv6 Source Guard on a VLAN 3
1.5.1 Configuration Tasks 3
1.5.2 Enabling IPv6 Source Guard on a VLAN 3
1.5.3 Configuring a Trusted Interface 4
1.5.4 Configuring an Untrusted Interface 4
1.6 Monitoring 4

1 Configuring IPv6 Source Guard

1.1 Introduction

1.1.1 Overview

The IPv6 Source Guard function enables the hardware to filter IPv6 packets to ensure that only users whose IPv6 packets match information in the database of the hardware can access the network normally, preventing users from privately setting IPv6 addresses or forging IPv6 packets.

1.1.2 Principles

1. Basic Concepts

- Source IPv6 address

  Indicate the source IPv6 address field in IPv6 packets.

- Source MAC address

  Indicate the source media access control (MAC) address field in L2 packets.

- User record binding database

  The user record binding database is the basis for IPv6 Source Guard. Data in the user record binding database comes from the following two sources:

  - Dynamic Host Configuration Protocol version 6 (DHCPv6) and neighbor discovery (ND) Snooping binding databases: After IPv6 Source Guard is enabled, information in the DHCPv6 and ND Snooping binding databases is synchronized to the user binding database of IPv6 Source Guard. In this case, IPv6 packets are filtered strictly through IPv6 Source Guard on devices with DHCPv6 or ND Snooping enabled. DHCPv6 Snooping and ND Snooping are two independent functions. Users can enable both functions or either function.
  - Static user configuration: including static user information bound by running the **ipv6 source binding** command and local link addresses (fe80::/10) and undefined addresses (::/128) released by running the **ipv6 verify source permit link-local** command.

2. Checking the Source Address Fields of Packets

IPv6 packets passing through an interface are checked based on the source IPv6 address or source IPv6 address and MAC address to prevent malicious users from forging packets to launch attacks.

When IPv6 Source Guard is enabled on an interface, the device checks the source addresses of packets passing through the interface, which can be a switching interface, L2 aggregation port (link aggregation), or L2 encapsulation subinterface. Only the packets whose source addresses match entries in the user record binding database can pass through the interface. There are two matching methods:

- Filtering based on the source IPv6 address

  The source IPv6 addresses of all IPv6 packets passing through an interface are checked. Only the packets whose source IPv6 addresses match entries in the user record binding database can pass through the interface. It is the default filtering policy of IPv6 Source Guard.

- Filtering based on the source IPv6 address and MAC address

  The source IPv6 addresses and MAC addresses of IPv6 packets passing through an interface are checked. Packets are allowed to pass through the interface only when both the L2 source MAC addresses and L3 source IPv6 addresses of these packets match an entry in the user record binding database.

1.2 Restrictions and Guidelines

- Typically, IPv6 Source Guard needs to work with DHCPv6 Snooping or ND Snooping. Therefore, DHCPv6 Snooping or ND Snooping should also be enabled. DHCPv6 Snooping or ND Snooping can be enabled either before or after IP Source Guard is enabled.
- If DHCPv6 Snooping is enabled on a device, the device does not check DHCPv6 packets.
- If ND Snooping is enabled on a device, the device does not check ND packets.

1.3 Configuration Task Summary

Select any of the following configuration tasks to configure.

- Enabling IPv6 Source Guard on an Interface
- Enabling IPv6 Source Guard on a VLAN

1.4 Enabling IPv6 Source Guard on an Interface

1.4.1 Restrictions and Guidelines

IPv6 Source Guard depends on DHCPv6 Snooping or ND Snooping. Users need to enable IPv6 Source Guard on an untrusted interface of DHCPv6 Snooping or ND Snooping.

1.4.2 Prerequisites

At least DHCPv6 Snooping or DN Snooping is enabled. To enable DHCPv6 Snooping, run the **ipv6 dhcp snooping** command. To enable ND Snooping, run the **ipv6 nd snooping enable** command.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Add static user information to the IPv6 source address binding database.

ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

No static user information is added by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) (Optional) Enable the function of converting IPv6 source address binding entries to static MAC address entries.

ipv6 source binding sticky-mac

The function of converting IPv6 source address binding entries to static MAC address entries is disabled by default.

(6) (Optional) Enable local link address release on an interface.

ipv6 verify source permit link-local

The local link address release function is disabled on an interface by default.

This command can be configured only on L2 switching interfaces and L2 aggregation ports.

Generally, this command is configured in a DHCPv6-only scenario. In this scenario, fe80::/10 address cannot be obtained through DHCPv6.

(7) Enable IPv6 Source Guard on an interface.

ipv6 **verify source** [**port-security**]

IPv6 Source Guard is disabled on an interface by default.

1.5 Enabling IPv6 Source Guard on a VLAN

1.5.1 Configuration Tasks

Enabling IPv6 Source Guard on a VLAN includes the following tasks:

(1) Enabling IPv6 Source Guard on a VLAN

(2) Configuring a Trusted Interface

(3) (Optional) Configuring an Untrusted Interface

1.5.2 Enabling IPv6 Source Guard on a VLAN

1. Prerequisites

At least DHCPv6 Snooping or DN Snooping is enabled. To enable DHCPv6 Snooping, run the **ipv6 dhcp snooping** command. To enable ND Snooping, run the **ipv6 nd snooping enable** command.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Add static user information to the IPv6 source address binding database.

ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

No static user information is added by default.

(4) Enter the VLAN configuration mode.

vlan { *vlan-id* | **range** *vlan-range* }

(5) Enable IPv6 Source Guard on a VLAN.

ipv6 verify source [**port-security**]

IPv6 Source Guard is disabled on a VLAN by default.

1.5.3 Configuring a Trusted Interface

1. Introduction

To enable IPv6 Source Guard on a VLAN, configure the uplink interface as an IPv6 Source Guard trusted interface. On the IPv6 Source Guard trusted interface, IPv6 Source Guard is not performed.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the uplink interface as an IPv6 Source Guard trusted interface.

ipv6 verify source trust

No interface is configured as an IPv6 Source Guard trusted interface by default.

1.5.4 Configuring an Untrusted Interface

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) The following configurations are optional. Please configure at least one task.

- Enable the function of converting IPv6 source address binding entries to static MAC address entries.

  ipv6 **source binding sticky-mac**

  The function of converting IPv6 source address binding entries to static MAC address entries is disabled by default.

- Enable local link address release on an interface.

  ipv6 **verify source permit link-local**

  The local link address release function is disabled on an interface by default.

  This command can be configured only on L2 switching interfaces and L2 aggregation ports.

  Generally, this command is configured in a DHCPv6-only scenario. In this scenario, fe80::/10 address cannot be obtained through DHCPv6.

1.6 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show ipv6 source binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**dhcp-snooping** | **static**]	Displays information of the IPv6 source address binding database.
show ipv6 source binding sticky-mac [**interface** *interface-type interface number*]	Displays information about IPv6 source address binding entries converted to static MAC address entries.

Contents

1 Configuring SAVI 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 2
1.2 Restrictions and Guidelines 2
1.3 Configuring SAVI 2
1.4 Monitoring 3
1.5 Configuration Examples 4
1.5.1 Configuring SAVI in an SLAAC-Only Scenario 4
1.5.2 Configuring SAVI in a DHCPv6-Only Scenario 5
1.5.3 Configuring SAVI in an SLAAC and DHCPv6 Deployment Scenario 7
1.6 Common Errors 8

1 Configuring SAVI

1.1 Introduction

1.1.1 Overview

Source Address Validation Improvement (SAVI) establishes a binding list based on the source IPv4/IPv6 addresses, source media access control (MAC) addresses, and access device ports for access devices through Control Packet Snooping (CPS) so as to verify the source addresses of IP packets through a specified port. The binding list sources include neighbor discovery (ND) Snooping, Dynamic Host Configuration Protocol version 6 (DHCPv6) Snooping, and static address configuration. Only packets whose source addresses match binding entries will be forwarded. This ensures the authenticity of source addresses of data packets in the network.

This document mainly describes the application of SAVI in IPv6 networks in stateful address configuration (DHCPv6 generally), stateless address autoconfiguration (SLAAC), and static address configuration scenarios.

1.1.2 Principles

1. Basic Concepts

- Source IPv6 address

  Indicate the source IPv6 address field in IPv6 packets.

- Source MAC address

  Indicate the source MAC address field in L2 packets.

- ND Snooping

  ND Snooping is used to snoop the SLAAC process of clients. The device with ND Snooping enabled extracts a client's IPv6 address and MAC address from a packet and generates a binding entry together with the port ID (interface index) and virtual local area network (VLAN) ID of the client.

- DHCPv6 Snooping

  DHCPv6 Snooping is used to snoop dynamical IPv6 address obtaining of clients through DHCPv6. The device with DHCPv6 Snooping enabled extracts a client's IPv6 address, MAC address, and lease from a packet and generates a binding entry together with the port ID (interface index) and VLAN ID of the client.

2. Checking the Source Address Fields of Packets

IPv6 packets passing through an interface are checked based on source IPv6 address or source IPv6 address and MAC address to prevent malicious users from forging packets to launch attacks.

When SAVI is enabled on an interface, the device checks the source addresses of packets passing through the interface, which can be a switching interface, L2 aggregation port (link aggregation), or L2 encapsulation subinterface. Only the packets whose source addresses match SAVI binding entries can pass through the interface. There are two matching methods:

- Filtering based on the source IPv6 address

  The source IPv6 addresses of all IPv6 packets passing through an interface are checked. Only the packets whose source IPv6 addresses match SAVI binding entries can pass through the interface.

- Filtering based on the source IPv6 address and MAC address

  The source IPv6 addresses and MAC addresses of all IPv6 packets passing through an interface are checked. Only the packets whose source IPv6 addresses and MAC addresses match SAVI binding entries can pass through the interface.

1.1.3 Protocols and Standards

- RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4861: Neighbor Discovery for IP version 6
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 6959: SAVI Threat Scope
- RFC 6620: FCFS SAVI Improvement for Locally Assigned IPv6 Addresses
- RFC 8074: SAVI for Mixed Address Assignment Methods Scenario
- RFC 7039: SAVI Framework
- RFC 7513: Solution for DHCP

1.2 Restrictions and Guidelines

- SAVI-related commands can be configured only after SAVI is enabled globally.
- Typically, SAVI needs to work with DHCPv6 Snooping or ND Snooping. Therefore, DHCPv6 Snooping or ND Snooping should also be enabled. DHCPv6 Snooping or ND Snooping can be enabled either before or after SAVI is enabled.
- If DHCPv6 Snooping is enabled on a device, the device does not check DHCPv6 packets.
- If ND Snooping is enabled on a device, the device does not check ND packets.
- Typically, SAVI is not enabled on DHCPv6 Snooping and ND Snooping trusted interfaces.
- After SAVI is enabled on an interface, the interface will deny all data packets whose source IPv6 addresses are not in the binding list. For control packets, only ICMPv6 packets of types 133, 134, 135, 136, 137, and 143 are permitted.
- After SAVI is enabled on an interface, the permit rules of IPv6 packets are related to the IPv6 address binding mode of global IP address and MAC address binding. The default address binding mode is the strict mode. In this mode, if IPv4 SAVI is enabled but IPv6 SAVI is disabled on an interface, all IPv6 packets through the interface will be intercepted. When IPv4 SAVI is enabled but IPv6 SAVI is disabled on all interfaces, it is recommended that the IPv6 address binding mode of global IP address and MAC address binding be set to the loose mode.

1.3 Configuring SAVI

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Add static user information to the IPv6 source address binding database.

savi ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-type interface-number* | **ip-mac** | **ip-only** }

No static user information is added by default.

(4) (Optional) Configure the data source of SAVI binding entries.

savi ipv6 bind-source add { **slaac** | **dhcp** }

Binding entries generated during the SLAAC and DHCPv6 processes are used as the sources of dynamic binding entries by default. Binding entries can also be statically configured.

(5) (Optional) Configure SAVI to permit local link addresses and undefined addresses.

savi ipv6 check permit link-local

Permitting local link addresses and undefined addresses is not configured by default.

After configuration, SAVI permits all IPv6 packets with fe80::/10 and ::/128 as source addresses.

Generally, this command is configured in a DHCPv6-only scenario. In this scenario, fe80::/10 address cannot be obtained through DHCPv6.

(6) (Optional) Enable binding entry migration.

savi ipv6 station-move

The binding entry migration function is disabled by default.

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Enable IPv6 SAVI.

savi ipv6 check source ip-address [**mac-address**]

IPv6 SAVI is disabled by default.

(9) (Optional) Configure the excluded VLANs for SAVI on an interface.

savi ipv6 check source exclude-vlan *vlan-id*

No excluded VLANs for SAVI are configured on an interface by default.

After SAVI is enabled on an interface, you can run this command to permit IPv6 packets of some VLANs.

1.4 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show savi ipv6 source binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**type** { **static** | **dhcp** | **slaac** }]	Displays information of the IPv6 source address binding database.
show savi ipv6 check source [*ipv6-address* | **interface** *interface-type interface-number*]	Displays effective IPv6 SAVI filtering entries.

1.5 Configuration Examples

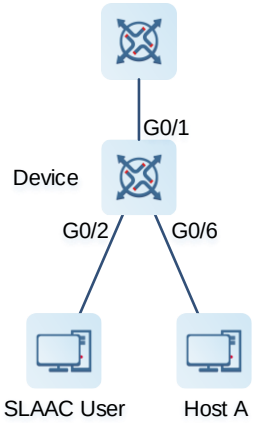
1.5.1 Configuring SAVI in an SLAAC-Only Scenario

1. Requirements

Enterprise devices connect to user hosts. No DHCPv6 server is deployed in the network, and hosts can obtain IPv6 addresses only through SLAAC. To prevent attackers from sending invalid IPv6 packets (including ND packets and IPv6 data packets), users need to filter out IPv6 packets with invalid source addresses.

2. Topology

Figure 1-1 Configuring SAVI in an SLAAC-Only Scenario



3. Notes

- Enable ND Snooping.
- Enable SAVI.

4. Procedure

Enable ND Snooping.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ipv6 nd snooping trust
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# ipv6 nd snooping enable
```

Enable SAVI.

```
Device(config)# interface gigabitethernet 0/2
Device(config-if-GigabitEthernet 0/2)# savi ipv6 check source ip-address mac-
address
Device(config-if-GigabitEthernet 0/2)# exit
Device(config)# interface gigabitethernet 0/6
```

```
Device(config-if-GigabitEthernet 0/6)# savi ipv6 check source ip-address mac-
address
```

5. Verification

Run the **show savi ipv6 check source** command to check SAVI filtering entries.

6. Configuration Files

Device configuration file

```
hostname Device
!
ipv6 nd snooping enable
!
interface GigabitEthernet 0/1
 ipv6 nd snooping trust
!
interface GigabitEthernet 0/2
 savi ipv6 check source ip-address mac-address
!
interface GigabitEthernet 0/6
 savi ipv6 check source ip-address mac-address
!
end
```

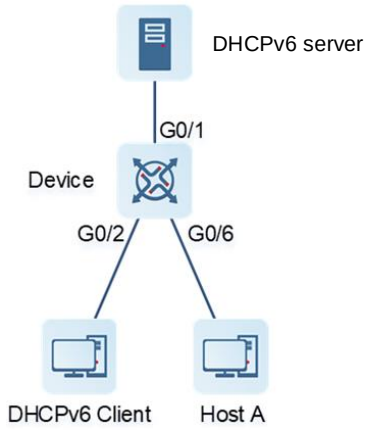
1.5.2 Configuring SAVI in a DHCPv6-Only Scenario

1. Requirements

Enterprise devices connect to user hosts. For unified IPv6 address management, hosts obtain IPv6 addresses through DHCPv6. To prevent attackers from sending invalid IPv6 packets (including DHCPv6 packets and IPv6 data packets), users need to filter out IPv6 packets with invalid source addresses.

2. Topology

Figure 1-2 Configuring SAVI in a DHCPv6-Only Scenario



3. Notes

- Enable DHCPv6 Snooping.
- Enable SAVI.

4. Procedure

Enable DHCPv6 Snooping.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ipv6 dhcp snooping trust
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# ipv6 dhcp snooping
```

Enable SAVI.

```
Device(config)# savi ipv6 check permit link-local
Device(config)# interface gigabitethernet 0/2
Device(config-if-GigabitEthernet 0/2)# savi ipv6 check source ip-address mac-
address
Device(config-if-GigabitEthernet 0/2)# exit
Device(config)# interface gigabitethernet 0/6
Device(config-if-GigabitEthernet 0/6)# savi ipv6 check source ip-address mac-
address
```

5. Verification

Run the **show savi ipv6 check source** command to check SAVI filtering entries.

6. Configuration Files

Device configuration file

```
hostname Device
!
ipv6 dhcp snooping
savi ipv6 check permit link-local
!
interface GigabitEthernet 0/1
 ipv6 nd snooping trust
!
interface GigabitEthernet 0/2
 savi ipv6 check source ip-address mac-address
!
interface GigabitEthernet 0/6
 savi ipv6 check source ip-address mac-address
!
end
```

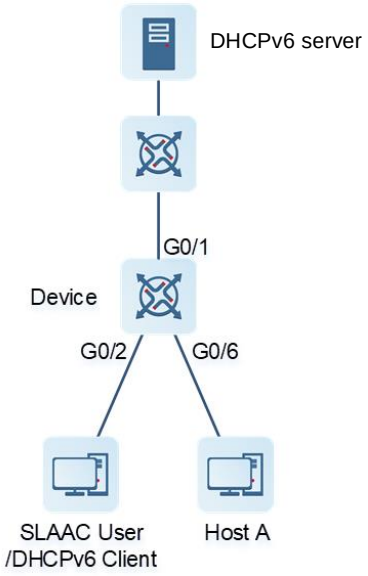
1.5.3 Configuring SAVI in an SLAAC and DHCPv6 Deployment Scenario

1. Requirements

Enterprise devices connect to user hosts. Some hosts obtain IPv6 addresses through SLAAC, and some hosts obtain IPv6 addresses through DHCPv6. To prevent attackers from sending invalid IPv6 packets (including DHCPv6 packets, ND packets, and IPv6 data packets), users need to filter out IPv6 packets with invalid source addresses.

2. Topology

Figure 1-3 Configuring SAVI in an SLAAC and DHCPv6 Deployment Scenario



3. Notes

- Enable ND Snooping and DHCPv6 Snooping.
- Enable SAVI.

4. Procedure

Enable ND Snooping and DHCPv6 Snooping.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ipv6 nd snooping trust
Device(config-if-GigabitEthernet 0/1)# ipv6 dhcp snooping trust
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# ipv6 nd snooping enable
Device(config)# ipv6 dhcp snooping
```

Enable SAVI.

```
Device(config)# interface gigabitethernet 0/2
```

```
Device(config-if-GigabitEthernet 0/2)# savi ipv6 check source ip-address mac-address
Device(config-if-GigabitEthernet 0/2)# exit
Device(config)# interface gigabitethernet 0/6
Device(config-if-GigabitEthernet 0/6)# savi ipv6 check source ip-address mac-address
```

5. Verification

Run the **show savi ipv6 check source** command to check SAVI filtering entries.

6. Configuration Files

Device configuration file

```
hostname Device
!
ipv6 nd snooping enable
ipv6 dhcp snooping
!
interface GigabitEthernet 0/1
 ipv6 nd snooping trust
 ipv6 dhcp snooping trust
!
interface GigabitEthernet 0/2
 savi ipv6 check source ip-address mac-address
!
interface GigabitEthernet 0/6
 savi ipv6 check source ip-address mac-address
!
end
```

1.6 Common Errors

SAVI is enabled on a DHCPv6 Snooping/ND Snooping trusted interface.

Contents

1 Configuring ARP Check 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.1.3 Protocols and Standards 1

1.2 Restrictions and Guidelines 1

1.3 Configuring ARP Check 2

1.4 Monitoring 2

1 Configuring ARP Check

1.1 Introduction

1.1.1 Overview

Address Resolution Protocol (ARP) Check is used to filter all ARP packets through an interface (L2 switching interface, L2 aggregation port, or L2 encapsulation subinterface) and discard all invalid ARP packets to prevent ARP spoofing and improve network stability.

On devices supporting ARP check, invalid ARP packets in networks will be filtered out according to the legitimate user information (detection based on IP address or IP address and MAC address) generated by security application modules such as IP Source Guard, global IP address and MAC address binding, 802.1x authentication, web authentication, and port security.

ARP Check uses the information to detect whether the Sender IP fields or the <Sender IP, Sender MAC> fields in all ARP packets through an interface match those in the legitimate user information table. If not, the ARP packets will be discarded.

1.1.2 Principles

1. Compatible Security Modules

ARP Check supports the following security modules:

- Detection of the IP address field only: port security and static configuration of IP Source Guard.
- Detection of the IP address and MAC address fields: IP Source Guard, global IP address and MAC address binding, 802.1x IP authorization, web authentication, and port security.

2. Filtering out Invalid ARP Packets

Enable ARP Check on specified interfaces to filter out invalid ARP packets.

A device matches the source IP and source MAC addresses of the ARP packets received through its interfaces with the valid user information in the database. With successful matching, packets will be transferred, or otherwise they will be discarded.

1.1.3 Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

1.2 Restrictions and Guidelines

- When ARP Check is enabled on an interface but IP Source Guard, global IP address and MAC address binding, 802.1x authentication, web authentication, or port security is not enabled on the interface to provide legitimate user information, all ARP packets through the interface will be discarded.
- ARP Check cannot be configured on mirrored destination ports.
- ARP Check cannot be configured on the trusted interfaces of DHCP Snooping.
- ARP Check cannot be configured on excluded interfaces of global IP address and MAC address binding.

- ARP Check can be configured only on switching interfaces, L2 aggregation ports, and L2 encapsulation subinterfaces.
- When ARP Check is enabled, the number of policies or users of related security applications may decrease.
- When the ARP Check and Virtual Router Redundancy Protocol (VRRP) functions are enabled on an interface and the physical IP address and virtual IP address of the interface can be used as the gateway address, the physical IP address and VRRP IP address need to be permitted to pass. Otherwise, ARP packets sent to the gateway will be filtered out.

1.3 Configuring ARP Check

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable ARP Check.

arp-check

ARP Check is disabled by default.

1.4 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show interfaces [*interface-type interface-number*] **arp-check list**	Displays the effective ARP Check entries on an interface.

Contents

1 Configuring DAI 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 1
1.2 Configuring DAI 2
1.2.1 Restrictions and Guidelines 2
1.2.2 Procedure 2
1.3 Monitoring 2
1.4 Configuration Examples 3
1.4.1 Requirements 3
1.4.2 Topology 3
1.4.3 Notes 3
1.4.4 Procedure 3
1.4.5 Verification 4
1.4.6 Configuration Files 4
1.4.7 Common Errors 5

1 Configuring DAI

1.1 Introduction

1.1.1 Overview

Dynamic ARP Inspection (DAI) is used to check the validity of received Address Resolution Protocol (ARP) packets and discard invalid ARP packets to prevent ARP spoofing and improve network stability. DAI generates ARP filtering information based on the legitimate user information (IP address or IP address and MAC address) generated by security application modules, such as IP Source Guard, global IP address and MAC address binding, 802.1x authentication, web authentication, and port security to filter out invalid ARP packets in the network.

1.1.2 Principles

1. Interface Trust Status

A device processes ARP packets based on the trust status of each interface. It regards ARP packets received through trusted interfaces as valid and does not perform DAI on such packets, and strictly performs DAI on packets received through untrusted interfaces.

In a typical network, L2 interfaces connected to network devices should be set as trusted interfaces, and L2 interfaces connected to hosts should be set as untrusted interfaces.

Notice

- After DAI is enabled, it is recommended that the uplink interfaces be configured as DAI trusted interfaces. If the uplink interfaces are not DAI trusted interfaces but trusted interfaces of other security functions, ARP packets will be filtered out because the interfaces do not have entries required for DAI.
- If another access security control command is configured on an interface, the interface cannot be configured as a DAI trusted interface. To set the interface as a DAI trusted interface, disable the configured security control command.

2. Filtering out Invalid ARP Packets

Due to defects of ARP, ARP cannot check the validity of received ARP packets. Attackers can easily use vulnerabilities of the protocol to launch ARP spoofing.

When DAI is enabled on a specified virtual local area network (VLAN), a device will intercept all ARP requests and responses transmitted through untrusted interfaces. The device matches the source IP addresses and media access control (MAC) addresses of the ARP packets received through its interfaces with the valid user records in the security database. With successful matching, packets will be transferred, or otherwise they will be discarded.

1.1.3 Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

1.2 Configuring DAI

1.2.1 Restrictions and Guidelines

- DAI cannot be enabled for Dynamic Host Configuration Protocol (DHCP) Snooping trusted interfaces in a VLAN.
- When DAI is disabled, it does not take effect to all interfaces in a VLAN. When ARP Check is still effective on an interface, the device will check ARP packets transmitted through the interface.
- DAI has the same functions as ARP Check. The only difference is that DAI is enabled for VLANs, and ARP Check is enabled for interfaces.

1.2.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DAI on a VLAN.

ip arp inspection vlan { *vlan-id* | *word* }

DAI is disabled on all VLANs by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure L2 interfaces as DAI trusted interfaces.

ip arp inspection trust

L2 interfaces are DAI untrusted interfaces by default.

(6) Configure the ARP packet receiving rate.

For details, see the rate limit command of NFPP.

1.3 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show ip arp inspection vlan [*vlan-id* | *vlan-range*]	Displays whether DAI is enabled for a VLAN.
show ip arp inspection interface	Displays the DAI configuration status on L2 interfaces.

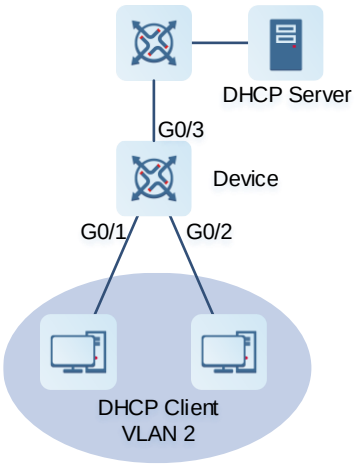
1.4 Configuration Examples

1.4.1 Requirements

Hosts can use only addresses assigned by a legitimate DHCP server to prevent ARP spoofing.

1.4.2 Topology

Figure 1-1 Configuring DAI



1.4.3 Notes

- Enable DHCP Snooping on the access device and set the interface (GigabitEthernet 0/3 in this example) connected to the legitimate DHCP server as a trusted interface.
- Enable IP Source Guard on the access device.
- Enable DAI after DHCP Snooping and IP Source Guard are enabled.

1.4.4 Procedure

Enable DHCP Snooping and IP Source Guard.

```
Device> enable
Device# configure terminal
Device(config)# interface range gigabitEthernet 0/1-2
Device(config-if-range)# switchport access vlan 2
Device(config-if-range)# ip verify source
Device(config-if-range)# exit
Device(config)# ip dhcp snooping
```

Configure DAI.

```
Device(config)# ip arp inspection vlan 2
```

Configure the trusted interface.

```
Device(config)# interface gigabitethernet 0/3
Device(config-if-GigabitEthernet 0/3)# switchport access vlan 2
Device(config-if-GigabitEthernet 0/3)# ip dhcp snooping trust
```

```
Device(config-if-GigabitEthernet 0/3)# ip arp inspection trust
```

1.4.5 Verification

Check whether DHCP Snooping, IP Source Guard and DAI are enabled, and whether the trusted interface is correct.

```
Device# show ip dhcp snooping
Switch DHCP snooping status                  :   ENABLE
DHCP snooping verify hardware address status    :   DISABLE
DHCP snooping database write-delay time        :   0 seconds
DHCP snooping option 82 status                :   DISABLE
DHCP snooping Support bootp bind status        :   DISABLE

Interface                    Trusted        Rate limit (pps)
------------------------       -------        ----------------
GigabitEthernet 0/3           YES           unlimited
Default                      No            unlimited
Device# show ip verify source
NO.   INTERFACE               FilterType FilterStatus         IPADDRESS
MACADDRESS    VLAN TYPE
----- ------------------------- ---------- ---------------------  ---------------
-------------- ---- -------------
1    GigabitEthernet 0/1      IP-ONLY   Active               Deny-All
2    GigabitEthernet 0/2      IP-ONLY   Active               Deny-All

Total number of bindings: 2
Device# show ip arp inspection vlan
Vlan Configuration
---- -------------
2   Enable
```

1.4.6 Configuration Files

```
hostname Device
!
ip arp inspection vlan 2
ip dhcp snooping
!
interface GigabitEthernet 0/1
 switchport access vlan 2
 ip verify source
!
interface GigabitEthernet 0/2
 switchport access vlan 2
 ip verify source
!
interface GigabitEthernet 0/3
 switchport access vlan 2
```

```
 ip arp inspection trust
 ip dhcp snooping trust
!
end
```

1.4.7 Common Errors

An interface configured with security limitations is set as a DAI trusted interface.

Contents

1 Configuring Gateway-targeted ARP Spoofing Prevention 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.1.3 Protocols and Standards 2

1.2 Configuring Gateway-targeted ARP Spoofing Prevention 2

1.3 Monitoring 2

1.4 Configuration Examples 2

1.4.1 Requirements 2

1.4.2 Topology 3

1.4.3 Notes 3

1.4.4 Procedure 3

1.4.5 Verification 3

1.4.6 Configuration Files 3

1 Configuring Gateway-targeted ARP Spoofing Prevention

1.1 Introduction

1.1.1 Overview

Due to defects of Address Resolution Protocol (ARP), ARP cannot check the validity of received ARP packets. Attackers can easily use vulnerabilities of the protocol to launch ARP spoofing. When a malicious user host is disguised as the gateway to send ARP packets, other user hosts in the network will learn false gateway ARP entries, resulting in ARP spoofing.

The gateway-targeted ARP spoofing prevention function is therefore used.

1.1.2 Principles

1. Basic Concepts

- ARP

  ARP is a Transmission Control Protocol (TCP)/IP protocol that obtains physical addresses according to IP addresses. A host broadcasts ARP requests to all hosts in the network and receives the returned packets to determine physical addresses of the target IP addresses, and saves the IP addresses and hardware addresses in the local ARP cache, which can be directly queried in response to future requests. In the same network, all the hosts using ARP are considered as mutually trustful to each other. Each host in the network can independently send ARP response packets, and the other hosts receive the response packets and record them in the local ARP cache without detecting their authenticity. In this way, attackers can send forged ARP response packets to target hosts so that the messages sent from these hosts cannot reach the proper host or reach a wrong host, thereby causing ARP spoofing.

- Gateway-targeted ARP spoofing

  When host A sends an ARP packet requesting the media access control (MAC) address of a gateway, host B on the same VLAN also receives this packet. Host B can send an ARP response packet, passing off the gateway IP address as the source IP address of the packet and host B's MAC address as the source MAC address. This is called gateway-targeted ARP spoofing. After receiving the ARP response, host A regards host B as the gateway. Therefore, all the packets sent from host A to the gateway during communication will be sent to host B. In this way, host A's communications are intercepted, causing ARP spoofing.

2. Gateway-targeted ARP Spoofing Prevention

Gateway-targeted ARP spoofing prevention is used to check whether the source IP address of an ARP packet through an access interface is set to the gateway IP address. If yes, the packet will be discarded to prevent hosts from receiving wrong ARP response packets. If not, the packet will not be handled. In this way, only the uplink devices can send ARP packets, and the ARP response packets sent from other PCs which pass for the gateway are filtered out.

1.1.3 Protocols and Standards

- RFC 826: Ethernet Address Resolution Protocol

1.2 Configuring Gateway-targeted ARP Spoofing Prevention

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable gateway-targeted ARP spoofing prevention.

anti-arp-spoofing ip *ipv4-address*

Gateway-targeted ARP spoofing prevention is disabled by default.

Gateway-targeted ARP spoofing prevention is supported only on L2 interfaces.

1.3 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show anti-arp-spoofing	Displays all data on gateway-targeted ARP spoofing prevention.

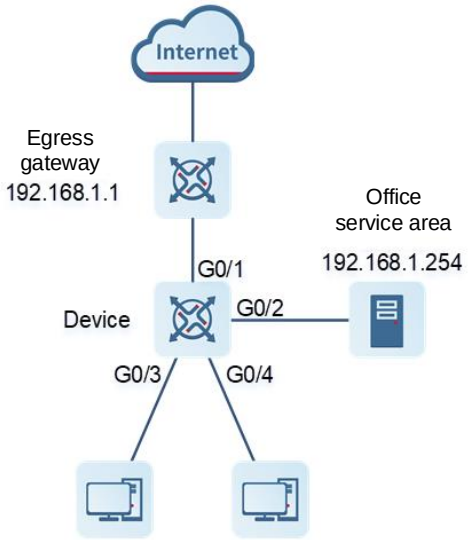
1.4 Configuration Examples

1.4.1 Requirements

User hosts access the office server through the access device, and connect to external networks through the gateway. If any malicious user hosts use forged gateway IP addresses or server IP addresses to perform ARP spoofing, the other user hosts cannot access the Internet or the server. The ARP spoofing packets with forged gateway addresses and intranet server IP addresses must be blocked so that users can access the Internet.

1.4.2 Topology

Figure 1-1 Configuring Gateway-targeted ARP Spoofing Prevention



1.4.3 Notes

Enable gateway-targeted ARP spoofing prevention on the access interface.

1.4.4 Procedure

Configure gateway-targeted ARP spoofing prevention.

```
Device> enable
Device# configure terminal
Device(config)# interface range gigabitEthernet 0/3-4
Device(config-if-range)# anti-arp-spoofing ip 192.168.1.1
Device(config-if-range)# anti-arp-spoofing ip 192.168.1.254
```

1.4.5 Verification

Run the **show anti-arp-spoofing** command to check for data on gateway-targeted ARP spoofing prevention.

```
Device> enable
Device# show anti-arp-spoofing
NO    PORT      IP              STATUS
----- ---------- ---------------- ----------
1     Gi0/3     192.168.1.1     active
2     Gi0/3     192.168.1.254    active
3     Gi0/4     192.168.1.1     active
4     Gi0/4     192.168.1.254    active
```

1.4.6 Configuration Files

```
hostname Device
!
```

```
interface GigabitEthernet 0/3
 anti-arp-spoofing ip 192.168.1.1
 anti-arp-spoofing ip 192.168.1.254
!
interface GigabitEthernet 0/4
 anti-arp-spoofing ip 192.168.1.1
 anti-arp-spoofing ip 192.168.1.254
!
end
```

Contents

1 Configuring CPP....1
1.1 Introduction....1
1.1.1 Basic Concepts....1
1.1.2 Processing Process....2
1.2 Configuration Task Summary....3
1.3 Configuring Basic Attributes of CPP....3
1.3.1 Overview....3
1.3.2 Restrictions and Guidelines....4
1.3.3 Procedure....4
1.4 Configuring Alarm Print Function of CPP....5
1.4.1 Overview....5
1.4.2 Restrictions and Guidelines....5
1.4.3 Procedure....5
1.5 Configuring Automatic Protection Function....6
1.5.1 Overview....6
1.5.2 Restrictions and Guidelines....6
1.5.3 Procedure....6
1.6 Configuring Automatic Protection Function for Ports....7
1.6.1 Overview....7
1.6.2 Restrictions and Guidelines....7
1.6.3 Procedure....8
1.7 Monitoring....9

1.8 Configuration Examples.....10

1.8.1 Configuring Basic Functions of CPP 10

1 Configuring CPP

1.1 Introduction

Many malicious attacks exist in the network environment. CPU attack packets significantly increase the CPU usage of a device, which affects the CPU to process and respond to the CPU to normal services and thus causes device function exceptions. CPU protect policy (CPP) protects the CPU of a device. By controlling the traffic of different types of packets sent to the CPU of the device and scheduling their priorities, users can defend against malicious attacks in the network and ensure that the CPU processes normal protocol packets.

1.1.1 Basic Concepts

1. QoS

As a network security mechanism, Quality of Service (QoS) is a technology that is used to solve network delay and congestion.

Differentiated Service (DiffServ) is a typical model of QoS that provides different services to packets by classifying service streams.

2. Bandwidth

Bandwidth specifies the maximum data transmission rate and the rate threshold for packet transmission in this document. When the data transmission rate exceeds the bandwidth, packets beyond the bandwidth are discarded. Therefore, the transmission rates of different types of packets must be equal to or smaller than the bandwidth. Both the bandwidth and data transmission rate use the unit of packets per second (pps).

3. L2/L3/L4

L2/L3/L4 means a hierarchical structure of packets based on the TCP/IP model. L2 means layer-2 headers, namely, the Ethernet encapsulation part; L3 means layer-3 headers, namely, the IP encapsulation part; L4 means layer-4 headers, usually, the TCP/UDP encapsulation part.

4. Priority Queue

The strict priority (SP) queue scheduling algorithm is a QoS scheduling algorithm. This scheduling algorithm requires packets to be processed based on the queue priority from high to low. The CPU must process first the packets in a high-priority queue and then those in a low-priority queue.

Packets to be sent to the CPU are cached in the SP queue and scheduled according to the algorithms of the SP queue. Packet scheduling is the process of selecting and transmitting packets in a priority queue to the CPU.

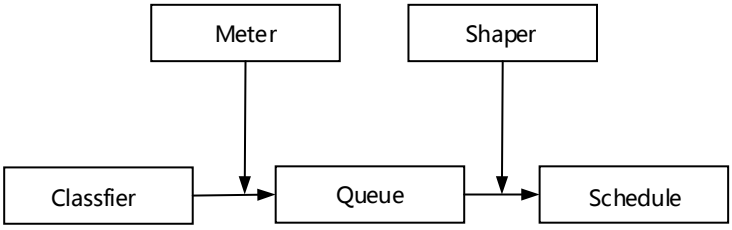
5. CPU Interface

A device caches packets before it sends them to the CPU. Sending the packets to the CPU is similar to a packet output process from the port. The CPU port is a virtual port through which packets are sent to the CPU. The priority queue and SP queue scheduling algorithms apply to only data packets that are transmitted through this CPU port.

1.1.2 Processing Process

The CPP function protects the CPU by using the standard QoS DiffServ model.

Figure 1-1 CPP Implementation Model



1. Classifier

The classifier classifies all packets to be sent to the CPU by the L2, L3 and L4 information of the packets. Classifying packets is the basis for implementing QoS policies. In subsequent actions, CPP can, according to the classification, implement different policies and provide different services. Packets on a device are classified by the supported protocols and management functions, for example, Bridge Protocol Data Unit (BPDU) packets of Spanning Tree Protocol (STP) and packets of Internet Control Message Protocol (ICMP). Packet types cannot be customized.

Instruction

Packet classification varies with products due to hardware difference. For details, see *Specifications* for details.

2. Meter

The meter limits the rates of different types of packets based on the set rate thresholds. You can set different rate thresholds for various packet types. When the rate of a packet type exceeds the threshold, the packets beyond the threshold are discarded.

By using the meter, you can control the rate of a packet type sent to the to the CPU within a threshold to prevent specific attack packets from exerting great impacts on the CPU resources. This is the level-1 protection of CPP.

3. Queue

Queues are used to classify packets at level 2. You can select the same queue for different packet types; queues cache packets in a device and provide services for the scheduler and shaper.

CPP queues are SP queues. The SPs of the packets are determined based on the time when they are added to a queue. Packets with a larger queue number have a higher priority.

4. Scheduler

The scheduler schedules packets based on SPs of queues. Packets in a high-priority queue are first scheduled.

Before being scheduled, the packets to be sent to the CPU are cached in queues. When being scheduled, the packets are sent to the CPU for processing.

Instruction

Only the SP scheduling policy is supported and cannot be modified.

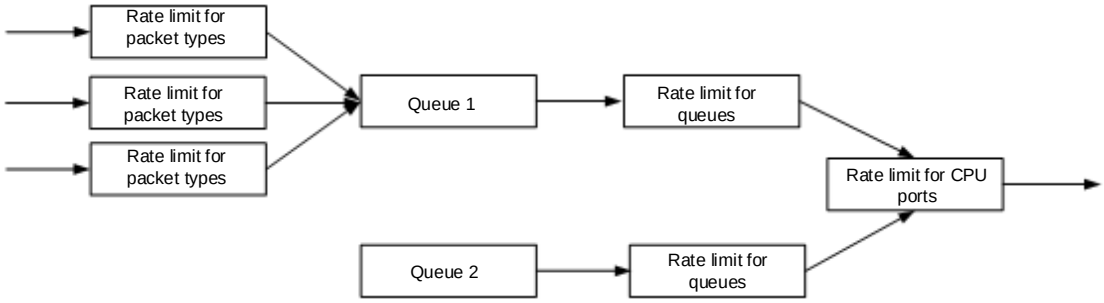
5. Shaper

The shaper shapes the packets to be sent to the CPU. When the actual rate of packets is greater than the shaping threshold, the packets must continue to cache in the queue and cannot be scheduled. When packet rates fluctuate, the shaper ensures that the rates of packets sent to the CPU are smooth (not more than the shaping threshold).

When the shaper is available, packets in a low-priority queue may be scheduled before those in a high-priority queue. If the rate of packets in a queue with a priority exceeds the shaping threshold, scheduling of the packets in this queue is stopped temporarily. Therefore, the shaper can prevent only the packets in high-priority queues from being scheduled.

Since the shaper limits the scheduling rates of packets, it provides the rate limit function. The shaper provides level-2 rate limit for priority queues and all packets sent to the CPU (CPU port). The shaper and meter functions provide 3-level rate limit and level-3 protection for the CPU.

Figure 1-2 3-Level Rate Limit of CPP



1.2 Configuration Task Summary

CPP configuration includes the following tasks:

- Configuring Basic Attributes of CPP
- Configuring Alarm Print Function of CPP
- Configuring Automatic Protection Function
- Configuring Automatic Protection Function for Ports

1.3 Configuring Basic Attributes of CPP

1.3.1 Overview

The implementation model of CPP includes five basic functional components: classifier, meter, queue, scheduler, and shaper. A device uses fixed classification policies for the classifier and SP scheduling algorithms for the scheduler.

In different network scenarios, users can configure personalized CPPs based on the meter, queue, and shaper to prevent packet attacks and network flapping from affecting normal operation of the CPU of a device.

- Configure a bandwidth for a specific packet type based on the meter to limit the packet transmission rate. Packets beyond the bandwidth are directly discarded.

- Configure a priority queue for a specific packet type based on the queue function. Packets in a high-priority queue are scheduled first.
- Configure a bandwidth for a CPU port and that for a specific priority queue to limit the packet transmission rate. Packets beyond the bandwidth are directly discarded.

1.3.2 Restrictions and Guidelines

- In one of the following situations, you must adjust the bandwidth for a specific packet type:
  - If a type of packets are discarded though they do not initiate attacks, you must increase the bandwidth for this packet type.
  - If a type of packets initiate attacks and cause CPU running exception, you must decrease the bandwidth for this packet type.
- In one of the following situations, you must adjust the priority queue for a specific packet type:
  - If a type of packets initiate attacks and cause exception in other packets in the same queue, you may put this type of packets into an unused queue.
  - A type of packets may not be discarded, and they are in the same queue with other types of packets in use. To prevent the bandwidth for other types of packets in the same queue from discarding packets, you can put this type of packets into a high-priority queue.
- In one of the following situations, you must adjust the bandwidth for a priority queue:
  - If the bandwidth for a type of packets increases, causing the available bandwidth for other packets in the same priority queue to decrease, you must appropriately increase the bandwidth for this priority queue.
  - If attack packets are put into a priority queue and no other packets in use stay in the same queue, you should decrease the bandwidth for this priority queue.
- When you configure a bandwidth for a specific packet type, note that decreasing the bandwidth may affect the normal service traffic of this packet type. To apply CPP based on users, use the NFPP function. For more information about NFPP configuration, see "Configuring Network Foundation Protection Policy".
- The bandwidth configuration for a packet type must match the bandwidth configuration for a priority queue. For the three levels of CPU protection, applying only one level of protection may cause negative effects. For example, if you increase the bandwidth for a packet type, you must also adjust the bandwidth for its priority queue. Otherwise, the other packets in the same priority queue may be affected.
- You are not advised to modify the bandwidth of the CPU port.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the basic attributes of CPP, and configure at least one task.

- Configure a bandwidth for a packet type.

  cpu-protect type *packet-type* **bandwidth** *bandwidth-value*

Each packet type has a rate threshold (bandwidth) by default, and this rate threshold may be modified, but may not be removed.

The default bandwidth for packet types depends on the actual product version.

- Configure a priority queue for a packet type.

  cpu-protect type *packet-type* **traffic-class** *traffic-class-number*

  Each packet type has a priority queue by default.

  The default priority queues for packet types depend on the actual product version.

- Configure a bandwidth for a priority queue.

  cpu-protect traffic-class *traffic-class-number* **bandwidth** *bandwidth-value*

  A shaping threshold (bandwidth) is determined for each priority queue by default, and this shaping threshold may be modified, but may not be removed.

  The default bandwidth for priority queues depends on the actual product version.

- Configure a bandwidth for the CPU interface.

  cpu-protect cpu bandwidth *bandwidth-value*

  The default bandwidth for the CPU port depends on the actual product version.

1.4 Configuring Alarm Print Function of CPP

1.4.1 Overview

After the alarm print function of CPP is enabled, you can view the alarm logs of lost packets and detect packet attacks to the CPU of the device timely. For the normal service packets that are discarded falsely, you can adjust the CPP configuration to avoid subsequent packet loss.

The configuration effect of the alarm print function is as follows:

- After the alarm print function is enabled for a packet type, the corresponding alarm log is printed if packets of this type are lost.
- After the alarm print function is enabled for a priority queue, the alarm log is printed if packets in this queue are lost.
- After an alarm period is configured, a device periodically detects the lost packets sent to the CPU, and the alarm is printed only once for the packet loss in this specified period.

1.4.2 Restrictions and Guidelines

- You can configure the alarm print function with two methods. Select either of them to validate this function. Commands configured between the configuration methods produce the same function effect. If they are configured, the later configured command takes effect. To facilitate management, you are advised to adopt one configuration method.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an alarm period of CPP. Please configure only one task.

- **cpu-protect alarm period** *period-value*
- **cpp-warn warn-period** *interval*

The default alarm period of CPP is **10** minutes.

(4) Enable the alarm print function for a packet type. Please configure only one task.

- **cpu-protect alarm type** *packet-type* **enable**
- **cpp-warn type** *packet-type* **warn**

The alarm print function for packets is not enabled by default.

(5) Enable the alarm print function for a queue. Please configure only one task.

- **cpu-protect alarm traffic-class** *traffic-class-number* **enable**
- **cpp-warn traffic-class** *traffic-class-number* **warn**

The alarm print function for priority queues is not enabled by default.

1.5 Configuring Automatic Protection Function

1.5.1 Overview

The automatic protection function allows a device to protect the application layer data based on sessions. The function ensures the normal operation of attacked services.

- After the automatic protection function is enabled based on packet types, the dynamic link protocol packets of the service module can get sufficient signaling to reduce protocol flapping when the packets are attacked.
- After it configures a domain for the customized security packet type, the function allows the matched security packets to get sufficient signaling to reduce protocol flapping when the packets are attacked.
- After it configures bandwidth for user trust packets, the function allows the trust packets to get sufficient signaling for forwarding, and limits the excessive bandwidth occupied by the packets.

1.5.2 Restrictions and Guidelines

- When the hardware capacity is insufficient, the whitelist entries configured by the Command Line Interface (CLI) or automatically delivered by services fail to be installed. A syslog is printed through the FP component on the device to indicate an entry capacity problem. Finally, the packet whitelist becomes invalid.
- You can enable the automatic protection function of protocol packets either in global configuration mode or for a packet type. If you do not configure the automatic protection function for a packet type, the global configuration of the automatic protection function prevails. If you configure the automatic protection function for a packet type, the configuration for this packet type prevails and the global configuration is not used.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the automatic protection function for protocol packets.

cpu-protect auto-defend [**type** *packet-type*] **enable**

When protocol flapping occurs frequently for a packet type, you can attempt to enable the automatic protection function for this packet type to prevent these packets from being affected by other protocol packets.

The automatic protection function for the dynamic routing protocol packets is disabled by default.

(4) Configure a trust packet type.

cpu-protect auto-defend trusted-host type *packet-type* { **src-ip** *ipv4-addres* | **src-ip6** *ipv6-address* | **src-mac** *mac-address* }

Each service is configured with a default trust packet type by default.

(5) Configure a bandwidth for packets under automatic protection.

cpu-protect auto-defend type *packet-type* **bandwidth** *value*

The bandwidth for trust packets under automatic protection is **80%** of the global bandwidth by default.

1.6 Configuring Automatic Protection Function for Ports

1.6.1 Overview

If a packet attack occurs on a port, the attack packets sent to the CPU through this port occupy bandwidth. As a result, other protocol packets cannot be sent to the CPU for processing and thus services are interrupted.

The automatic protection function can defend against packet attacks to CPU ports. The implementation effect is as follows:

- After the automatic protection function for a port is enabled, a device can detect packet attacks on this port.
- After it configures an automatic protection attack threshold for a port that transmits protocol packets, this function allows the packets to have sufficient signaling for forwarding and limits the excessive bandwidth occupied by the packets.
- After it configures a blacklist to impose a rate limiting threshold for the ports in the blacklist, this function allows service packets to get sufficient bandwidth on other ports.
- After it configures a monitoring period for a port, this function limits the rates of attack packets on this port within the period. After the period, this function limits the rates of attack packets if the protocol packets received on this port remain in excess of the attack threshold. Otherwise, the limit is removed.
- After the attack alarming function is enabled on a port, syslogs are generated and Simple Network Management Protocol (SNMP) Trap messages are sent when attacks occur or are cleared. The alarm message is triggered when they occur or are cleared. The alarm is not given repeatedly during a monitoring period.

1.6.2 Restrictions and Guidelines

- When the default hardware capacity is insufficient, the blacklist entries fail to be installed. A syslog is printed through the FP component on the device to indicate an entry capacity problem. Finally, the rate limit by the hardware may become ineffective and must be reconfigured by software.
- To detect a specific network environment, you can enable the packet statistics function on a port and check attacks based on the packet statistics. If any, enable the automatic protection function on the port and configure an attack threshold and a rate limiting threshold based on the environmental configuration.

- The blacklist can take effect on a port only when the automatic protection function is enabled on this port.
- You can enable the automatic protection function in global configuration mode or for a port. If you do not configure the automatic protection function for a port, the global configuration of the automatic protection function prevails. If you configure the automatic protection function for a port, the configuration for this port prevails and the global configuration is not used.
- You can configure the packet penalty threshold for an attacked port in global configuration mode or for a specific packet type. If you do not configure the penalty threshold for a specific packet type, you impose a penalty threshold on packets in the global configuration mode when an attack is detected on a port. If you configure a penalty threshold for a specific packet type, the configuration for this packet type prevails.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the automatic protection function for a port.

cpu-protect auto-port-defend [**interface** *interface-type interface-number* | **interface range** *interface-type start-number end-number*] **enable**

The automatic protection function for a port is disabled by default.

(4) Configure an attack threshold for a packet type under automatic protection on a port.

cpu-protect auto-port-defend type *packet-type* **attack-threshold** *threshold-value*

No attack threshold is configured for a packet type under automatic protection on a port by default.

(5) Configure a rate limiting threshold for all packets on an attacked port.

cpu-protect auto-port-defend limit threshold *threshold-value*

In the monitoring period, a rate limiting threshold will be applied to a port if an attack is detected on the port.

The rate limiting threshold for all packets on an attacked port is **5%** of the bandwidth for this interface by default.

(6) Configure a rate limiting threshold for specific packets on an attacked port.

cpu-protect auto-port-defend limit type *packet-type* **threshold** *threshold-value*

In the monitoring period, a rate limiting threshold is applied to the specific packets on a port if an attack is detected on the port.

The rate limiting threshold for specific packets on an attacked port is **5%** of the bandwidth for the port packets by default.

(7) Configure a blacklist for a port.

cpu-protect auto-port-defend blacklist interface *interface-type interface-number*

If a port that normally sends and receives packets is not identified as an attack interface, but affects traffic of services, you can add this port to a blacklist to reduce the traffic of this port.

A port is a trust port and is not in the blacklist by default.

(8) Configure a monitoring period for a port.

cpu-protect auto-port-defend monitor-period *value*

The default attack monitoring period of a port is **300** seconds.

(9) Enable the attack alarm function for a port.

cpu-protect auto-port-defend alarm enable

The attack alarm function for a port is disabled by default. After an attack occurs or is cleared, syslogs are not output and SNMP Trap messages are not sent to prompt users.

1.7 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Notice

- Running the **clear** command may lose vital information and thus interrupt services.
- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
clear cpu-protect counters [**device** *device-number*] [**slot** *slot-number*]	Clears CPP statistics.
clear cpu-protect counters mboard	Clears the CPP statistics on the master device.
clear cpu-protect statistics [**interface** *interface-type interface-number*]	Clears the CPP statistics on an interface.
show cpu-protect type *packet-type* [**device** *device-number*] [**slot** *slot-number*]	Displays the configuration and statistics of a packet type.
show cpu-protect traffic-class *traffic-class-number* [**device** *device-number*] [**slot** *slot-number*]	Displays the configuration and statistics of a priority queue.
show cpu-protect cpu	Displays the configuration on the CPU port.
show cpu-protect { **mboard** | **summary** }	Displays all the configuration and statistics on the master device.
show cpu-protect [**device** *device-number*] [**slot** *slot-number*]	Displays all the configuration and statistics of CPP.
show cpu-protect statistics [**interface** *interface-type interface-number*]	Displays the statistics on a CPP port.
show cpu-protect statistics type *packet-type*	Displays the statistics of a packet type on a CPP port.

Command	Purpose
show cpu-protect hardware-statistics [**device** *device-number*] [**slot** *slot-number*]	Displays the hardware statistics of a CPP packet type.
show cpu-protect auto-defend	Displays automatic protection configuration and whitelist packet statistics.
show cpu-protect auto-defend summary	Displays the automatic protection configuration.
show cpu-protect auto-defend config	Displays the trust packet configuration.
show cpu-protect auto-port-defend	Displays the blacklist configuration on a port.
show cpu-protect auto-port-defend statistics	Displays the blacklist statistics on a port.
show cpu-protect auto-port-defend summary	Displays the automatic protection configuration on a port.
show cpu-protect auto-port-defend attacked summary	Displays the packet attack information on a port.
show cpu-protect linkage summary	Displays the protocol correlation state.

Instruction

The above monitoring command is compatible with chassis devices and cassette devices, as well as the standalone mode and VSU mode.

If the **device** and **slot** keywords are not entered, the **clear** command is used to clear the statistics of all nodes and interfaces in the system and the **show** command is used to display the configuration on the master device.

In the stand-alone mode, the **device** keyword is invisible. For chassis devices, the **slot** keyword is used to specify a line card; for cassette devices, the **slot** keyword is invisible.

In the VSU mode, the **device** keyword specifies a chassis or cassette device. If the **device** keyword is not entered, it specifies the master chassis or the master device. For chassis devices, if the **device** keyword is entered, the **slot** keyword must also be entered to mark a line card in a chassis; for cassette devices, the **slot** keyword is invisible.

1.8 Configuration Examples

1.8.1 Configuring Basic Functions of CPP

1. Requirements

Address Resolution Protocol (ARP), IP, Open Shortest Path First (OSPF), dot1x, Virtual Router Redundancy Protocol (VRRP), Telnet and ICMP streams are available in the system. In the current configuration, ARP and dot1x streams are in priority queue 2; IP, ICMP and Telnet streams are in priority queue 4; OSPF streams are in priority queue 3; and VRRP streams are in priority queue 6. The bandwidth for each packet type is 10,000 pps; the bandwidth for each priority queue is 20,000 pps; and the bandwidth for the CPU port is 100,000 pps. If the

device suffers ARP packet attacks, you must enable the CPP function to prevent the packet attacks and network flapping and ensure the normal running of other services on the device.

2. Notes

- Classify ARP attack packets into priority queue 1 and limit the bandwidth for ARP packets or the priority queue.
- Classify OSPF packets into priority queue 5.
- Classify IP attack packets (without the ARP entries) into priority queue 3 and limit the bandwidth for IP packets or the priority queue.

3. Procedure

Configure the basic attributes of CPP.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# cpu-protect type arp traffic-class 1
DeviceA(config)# cpu-protect type arp bandwidth 5000
DeviceA(config)# cpu-protect type ospf traffic-class 5
DeviceA(config)# cpu-protect type v4uc-route traffic-class 3
DeviceA(config)# cpu-protect traffic-class 3 bandwidth 5000
DeviceA(config)# end
```

4. Verification

Run the **show cpu-protect** command to view the configuration and statistics.

```
DeviceA# show cpu-protect
%cpu port bandwidth: 100000(pps)
Traffic-class   Bandwidth(pps)  Rate(pps)  Drop(pps)
-------------   --------------  ---------  ---------
 0            20000          0         0
 1            20000          0         0
 2            20000          0         0
 3            5000           0         0
 4            20000          0         0
 5            20000          0         0
 6            20000          0         0
 7            20000          0         0
Packet Type        Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total
Total Drop
------------------  -------------  --------------  ---------  ---------  ---------
----------
bpdu              6            128           0         0         0           0
arp               1            5000          0         0         0           0
tpp               6            128           0         0         0           0
dot1x             2            1500          0         0         0           0
gvrp              5            128           0         0         0           0
rldp              5            128           0         0         0           0
```

lacp	5	256	0	0	0	0
rerp	5	128	0	0	0	0
reup	5	128	0	0	0	0
lldp	5	768	0	0	0	0
cdp	5	768	0	0	0	0
dhcps	2	1500	0	0	0	0
dhcps6	2	1500	0	0	0	0
dhcp6-client	2	1500	0	0	0	0
dhcp6-server	2	1500	0	0	0	0
dhcp-relay-c	2	1500	0	0	0	0
dhcp-relay-s	2	1500	0	0	0	0
option82	2	1500	0	0	0	0
tunnel-bpdu	2	128	0	0	0	0
tunnel-gvrp	2	128	0	0	0	0
unknown-v6mc	1	128	0	0	0	0
xgv6-ipmc	1	128	0	0	0	0
stargv6-ipmc	1	128	0	0	0	0
unknown-v4mc	1	128	0	0	0	0
xgv-ipmc	2	128	0	0	0	0
stargv-ipmc	2	128	0	0	0	0
udp-helper	1	128	0	0	0	0
dvmrp	4	128	0	0	0	0
igmp	2	1000	0	0	0	0
icmp	3	1600	0	0	0	0
ospf	5	2000	0	0	0	0
ospf3	5	2000	0	0	0	0
pim	4	1000	0	0	0	0
pimv6	4	1000	0	0	0	0
rip	4	128	0	0	0	0
ripng	4	128	0	0	0	0
vrrp	6	256	0	0	0	0
vrrpv6	6	256	0	0	0	0
ttl0	0	128	0	0	0	0
ttl1	0	2000	0	0	0	0
hop-limit	0	800	0	0	0	0
local-ipv4	3	4000	0	0	0	0
local-ipv6	3	4000	0	0	0	0
v4uc-route	3	800	0	0	0	0
v6uc-route	1	800	0	0	0	0
rt-host	4	3000	0	0	0	0
mld	2	1000	0	0	0	0
nd-snp-ns-na	1	3000	0	0	0	0
nd-snp-rs	1	1000	0	0	0	0
nd-snp-ra-redirect	1	1000	0	0	0	0
erps	5	128	0	0	0	0
mpls-ttl0	4	128	0	0	0	0

```
mpls-ttl1          4            128            0          0          0            0
mpls-ctrl          4            128            0          0          0            0
isis               4            2000           0          0          0            0
bgp                4            2000           0          0          0            0
cfm                5            512            0          0          0            0
web-auth           2            2000           0          0          0            0
fcoe-fip           4            1000           0          0          0            0
fcoe-local         4            1000           0          0          0            0
bfd                6            5120           0          0          0            0
micro-bfd          6            5120           0          0          0            0
micro-bfd-v6       6            5120           0          0          0            0
dldp               6            3200           0          0          0            0
other              0            4096           0          0          0            0
trill              4            1000           0          0          0            0
efm                5            1000           0          0          0            0
ipv6-all           0            2000           0          0          0            0
ip-option          0            800            0          0          0            0
mgmt               -            4000           4          0          4639         0
dns                2            200            0          0          0            0
sdn                0            5000           0          0          0            0
sdn_of_fetch       0            5000           0          0          0            0
sdn_of_copy        0            5000           0          0          0            0
sdn_of_trap        0            5000           0          0          0            0
vxlan-non-uc       1            512            0          0          0            0
local-telnet       3            1000           0          0          0            0
local-snmp         3            1000           0          0          0            0
local-ssh          3            1000           0          0          0            0
```

Contents

1 Configuring NFPP 1
1.1 Introduction 1
1.1.1 Basic Concepts 1
1.1.2 Rate Limiting Threshold and Attack Identification for Hosts 3
1.1.3 Rate Limiting and Attack Identification for Ports 3
1.1.4 Hardware Isolation 3
1.1.5 Monitoring Time 4
1.1.6 Trust Host 4
1.2 Configuration Task Summary 4
1.3 Configuring ARP Guard 4
1.3.1 Overview 4
1.3.2 Restrictions and Guidelines 5
1.3.3 Procedure (Global Configuration) 6
1.3.4 Procedure (Interface Configuration) 7
1.4 Configuring IP Guard 8
1.4.1 Overview 8
1.4.2 Restrictions and Guidelines 8
1.4.3 Procedure (Global Configuration) 9
1.4.4 Procedure (Interface Configuration) 10
1.5 Configuring TCP-SYN Guard 11
1.5.1 Overview 11
1.5.2 Restrictions and Guidelines 11

1.5.3 Procedure (Global Configuration) 12

1.5.4 Procedure (Interface Configuration) 12

1.6 Configuring ICMP Guard 13

1.6.1 Overview 13

1.6.2 Restrictions and Guidelines 13

1.6.3 Procedure (Global Configuration) 14

1.6.4 Procedure (Interface Configuration) 15

1.7 Configuring DHCP Guard 16

1.7.1 Overview 16

1.7.2 Restrictions and Guidelines 16

1.7.3 Procedure (Global Configuration) 17

1.7.4 Procedure (Interface Configuration) 17

1.8 Configuring DHCPv6 Guard 18

1.8.1 Overview 18

1.8.2 Restrictions and Guidelines 18

1.8.3 Procedure (Global Configuration) 19

1.8.4 Procedure (Interface Configuration) 20

1.9 Configuring ND Guard 20

1.9.1 Overview 20

1.9.2 Restrictions and Guidelines 20

1.9.3 Procedure (Global Configuration) 21

1.9.4 Procedure (Interface Configuration) 21

1.10 Customizing Guard 22

1.10.1 Overview 22

1.10.2 Restrictions and Guidelines 22

1.10.3 Procedure (Global Configuration) 24

1.10.4 Procedure (Interface Configuration) 25

1.11 Disabling Guard 25

1.11.1 Overview 25

1.11.2 Restrictions and Guidelines 25

1.11.3 Procedure 26

1.12 Configuring NFPP Logs 26

1.12.1 Overview 26

1.12.2 Restrictions and Guidelines 26

1.12.3 Procedure 26

1.13 Monitoring 27

1.14 Configuration Examples 29

1.14.1 Configuring CPU Guard 29

1 Configuring NFPP

1.1 Introduction

Many malicious attacks exist in the network environment. If no protection policies are available, attack packets occupy the CPU resources of a device. As a result, the CPU cannot process normal protocol packets and control packets and the device does not normally run. The network foundation protection policy (NFPP) protects devices from attacks and keeps a low CPU load for the devices under attack to ensure normal operation of services and stable operation of the entire network.

1.1.1 Basic Concepts

1. ARP Guard

In a LAN, the Address Resolution Protocol (ARP) can parse an IP address into a MAC address to ensure smooth communication. The Denial of Service (DoS) is a process of sending many invalid ARP packets to a gateway in a network to cause the gateway not to provide services for normal hosts. To avoid this type of attacks, configure a rate limiting threshold for the ARP packets and isolate the source of the attack.

2. IP Guard

Hacking attack and network virus intrusion start at a host that scans network activities. Many scanned packets occupy network bandwidth and thus affect normal communication of the network. To avoid this type of attacks, we configure the IP guard function for a device. This function also reduces the CPU usage of the device. IP attacks include the following two types:

- Scan changes in the destination IP address. This type of attacks consume network bandwidth and increase device load. This indicates most of upcoming hacking attacks.
- Send IP packets to an unconfigured destination IP address. This attack is designed for the CPU of a device. On an L3 device, if a destination IP address is configured, packets are forwarded by the chip without consuming CPU resources. Otherwise, the packets are sent to the CPU and the latter sends ARP requests to request the MAC address of the destination IP address. If too many packets sent to the CPU, this consumes many CPU resources. To avoid this type of attacks, we configure a rate limiting threshold for the IP packets and isolate the source of the attack.

3. TCP SYN Guard

TCP-SYN-Flood attack is also called half-open connection attack. An attacker sends SYN packets to the target device without responding to the SYN+ACK packets returned by the target device. If it does not receive the SYN+ACK responses, the target device waits and thus a half-open connection is formed. The attacker allows the target device to generate many half-open connections with this method, forcing the target device to waste resources on the half-open connections.

The available TCP connections of a server are limited. If a malicious attacker sends this type of connection requests consecutively in an attack, the available TCP connections of this server become congested. Thus, the available system resources and available bandwidth drop dramatically, affecting normal network services. Consequently, a DoS occurs.

To avoid the TCP-SYN-Flood attack, configure the TCP SYN guard function on the device to limit the sending rates of TCP SYN packets.

4. ICMP Guard

The Internet Control Message Protocol (ICMP) is a common means of network fault diagnosis. According to the principle of ICMP, when a host sends an ICMP Echo Request packet, the receiver returns an ICMP Echo Reply upon receipt of the packet. This process requires CPU coordination. If an attacker sends many ICMP requests to the target device, many CPU resources are consumed, which may interrupt normal device operation in extreme conditions. This is called an ICMP flood attack. To avoid it, configure a rate limiting threshold for the ICMP packets and isolate the source of the attack.

5. DHCP Guard

The Dynamic Host Configuration Protocol (DHCP) is widely used in a LAN to dynamically assign IP addresses. A DHCP starvation attack is the most popular DHCP attack that broadcasts DHCP requests by using a false MAC address. When a network attacker sends enough DHCP requests, it can exhaust the address space of the DHCP server within a period. In this case, the legal host fails to request IP addresses from the DHCP server and thus cannot access a network. To avoid this type of attacks, configure a rate limiting threshold for the DHCP packets and isolate the detected source of the attack.

6. DHCPv6 Guard

DHCPv6 is widely used in a LAN to dynamically assign IPv6 addresses. Like DHCPv4, DHCPv6 has security problems. Therefore, the attack methods of DHCPv4 are applicable to DHCPv6. When a network attacker sends enough DHCPv6 requests, it can exhaust the address space of the DHCPv6 server within a period. In this case, the legal host fails to request IPv6 addresses from the DHCP server and thus cannot access a network. To avoid this type of attacks, configure a rate limiting threshold for DHCPv6 packets and isolate the detected source of the attack.

7. ND Guard

Neighbor discovery (ND) parses addresses, discovers routes and prefixes, and redirects routes in an IPv6 network. A ND process involves five types of packets: Neighbor Solicitation (NS), Neighbor Advertisement (NA), Router Solicitation (RS), Router Advertisement (RA), and Redirect packets. The five types of packets are called ND packets collectively.

ND Snooping listens to ND packets in a network, filters out invalid ND packets, and monitors IPv6 users and binds these users to ports to avoid theft of IPv6 addresses. ND Snooping requires ND packets to be sent to the CPU. If they are sent at a high rate, this initiates an attack on the CPU. Therefore, we must configure ND guard to limit the rates of ND packets.

8. Customized Guard

There are many types of network protocols, including routing protocols such as OSPF, BGP, and RIP. To exchange packets between devices running different protocols, the packets must be sent to the CPU and processed by the protocol. Each protocol running on a device gives attackers a chance to initiate attacks. If an attacker sends many protocol packets to a network device, this consumes many CPU resources of the device, even affecting device operation.

Network protocols are diverse and grow constantly. Different protocols are demanded in different user environments. Therefore, protocol-specific guard functions have some limitations. To avoid this type of attacks,

configure the customized guard function for the device to allow users to flexibly define and configure guard types to meet guard requirements in different user environments.

1.1.2 Rate Limiting Threshold and Attack Identification for Hosts

By configuring a rate limiting threshold for attack packets of hosts, a device can identify different attack scenarios such as host attacks, ARP scanning, and IP scanning. Host attacks can be identified in the following ways:

- Identify hosts according to the source IP address, VLAN ID, and port.
- Identify hosts according to the source MAC address, VLAN ID, and port on the link layer.

Each host is configured with a rate limiting threshold and an attack or attack threshold. The rate limiting threshold must be smaller than the attack threshold.

- If a single host sends attack packets at a rate higher than the rate limiting threshold, packets out of the threshold are discarded.
- If a single host sends attack packets at a rate higher than the attack threshold, the host behavior is identified as an attack and recorded into the log. Meanwhile, a Trap message is sent.
- If the received ARP packets exceed the scanning threshold in the configured period, the source MAC address in the packets is unchanged and the source IP address is changing on the link layer, or the source MAC address and source IP address on the link layer are unchanged but the destination IP address is changing, an ARP scanning attack is suspected.
- If the received IP packets exceed the scanning threshold in the configured period and the source IP address in the packets is unchanged and the destination IP address is changing, an IP scanning attack is suspected.

Instruction

- When NFPP detects attacks of a specific packet type, NFPP can send an alarm message to users. To avoid frequent alarm messages, NFPP does not resend an alarm within 60 seconds running after the message is generated.
- To prevent frequent log printing from consuming CPU resources, NFPP writes attacks related log content into the buffer and prints the log content from the buffer at the specified rate. NFPP does not limit the rates of Trap messages.
- Only ARP guard and IP scanning guard support the scanning prevention function.

1.1.3 Rate Limiting and Attack Identification for Ports

Each port is configured with a rate limiting threshold and an attack threshold. The rate limiting threshold must be smaller than the attack threshold.

- If a single port sends packets at a rate higher than the rate limiting threshold, packets out of the threshold are discarded.
- If a single port sends packets at a rate higher than the attack threshold, the port behavior is recorded into the log. Meanwhile, a Trap message is sent.

1.1.4 Hardware Isolation

Hardware is isolated by the guard policy after an attack is detected. Isolation requires a filter of hardware. Attack packets from an isolated device are not sent to the CPU for processing to ensure normal operation of the device.

Hardware isolation falls into host based isolation and port-based isolation. The port-based isolation configures a rate limit for physical ports. Only ARP guard and ND guard support hardware isolation based on physical ports.

To isolate attackers, you must configure policies for hardware entries. Because hardware resources are limited, a log is printed to remind users when such resources are exhausted.

Instruction

Only ARP guard can be configured with the global isolation and forwarding function and the rate limit function for port-based isolation and forwarding.

1.1.5 Monitoring Time

Monitoring hosts can detect attacks in the system. If the isolation time is 0 (indicating no isolation), the guard module automatically monitors attackers through software based on the configured monitoring time. If the isolation time is not 0, the guard module isolates attackers through hardware.

During software monitoring, when the isolation time is configured as a non-zero value, the guard module automatically isolates the attackers under software monitoring through hardware and configures the timeout time of the software monitoring as the isolation time. The monitoring time takes effect only when the isolation time is 0.

1.1.6 Trust Host

To stop monitoring a host is to trust the host. You can configure the host as a trusted host to allow it to send packets to the CPU.

1.2 Configuration Task Summary

NFPP configuration includes the following tasks:

(1) Configuring ARP Guard

(2) Configuring IP Guard

(3) Configuring TCP-SYN Guard

(4) Configuring ICMP Guard

(5) Configuring DHCP Guard

(6) Configuring DHCPv6 Guard

(7) Configuring ND Guard

(8) Customizing Guard

(9) Disabling Guard

(10) Configuring NFPP Logs

1.3 Configuring ARP Guard

1.3.1 Overview

ARP guard is used to detect, process, and prevent ARP based packet attacks. It includes the following functions:

- Identify ARP attacks based on hosts or physical ports. This function can determine an attack host based on

the source IP address/MAC address (link layer), VLAN ID, and physical port. A rate limiting threshold and an attack threshold can be configured for each attack identification method. When the ARP packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the ARP packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent to remind users of ARP attacks.

- Identify ARP scanning attacks. For the ARP packets received within 10 seconds, if the source MAC address is unchanged and the source IP address is changing on the link layer, or the former and source IP address on the link layer are unchanged but the destination IP address is changing more than the specified scanning threshold of times, an ARP scanning attack is suspected and an alarm is printed to remind users.
- Isolate the source of ARP attacks based on hosts or ports.
  - This function configures hardware entries to isolate the identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
  - After isolation takes effect, you can enable the isolation forwarding function to limit the isolation range so that only the management plane of the target CPU is isolated and packets on the data plane are still forwarded.
  - If the port-based isolation entries take effect, the default action is to discard all attack packets. After you enable the function of port-based rate limit forwarding, you can allow some of packets to pass through by changing the isolation action.
- Monitor host attacks through software. After this function guard identifies any attacks, it can monitor the attack host through software in the configured monitoring time.

1.3.2 Restrictions and Guidelines

- ARP guard is to solve the ARP DoS attacks on a device. This function can reduce the impact of this type of attacks on the device, but does not cope with ARP spoofing attacks or ARP attacks in a network.
- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails. For example, if the ARP guard function is enabled on an interface and then disabled in global configuration mode, the function remains effective on this interface.
- After the ARP guard function is disabled, the system automatically clears the entries related to the monitored hosts, scanning hosts, and isolated ports.
- The rate limiting threshold configured based on a MAC address has a higher priority than that configured based on an IP address, and the rate limiting threshold configured based on an IP address has a higher priority than that configured based on a port. To optimize the ARP guard effect, users are advised to configure rate limiting thresholds and attack thresholds for hosts based on the following rules:
  Attack threshold based on source MAC address > Rate limiting threshold based on source MAC address > Attack threshold based on IP address > Rate limiting threshold based on IP address
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- An ARP scanning table can store only 256 latest records. When the ARP scanning table is full, new records overwrite old ones. ARP scanning attacks may be misjudged. Therefore, when ARP guard does not isolate a detected host that is suspected to initiate an ARP scanning attack, this function only provides some information for the reference of users.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure

isolation time to discard the packets and prevent them from occupying bandwidth. When you configure isolation time, you must note that:

- If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
- If you change the isolation time to 0 from a non-zero value, entries of the isolated attacker are directly deleted without monitoring the attacker through software.

- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.

1.3.3 Procedure (Global Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the NFPP configuration mode.

nfpp

(4) Enable the function of global ARP guard.

arp-guard enable

The function of global ARP guard is enabled by default.

(5) (Optional) Configure the global isolation time of ARP guard.

arp-guard isolate-period [*interval* | **permanent**]

The default global isolation time of ARP guard is **0**, and the isolation function is disabled by default.

(6) (Optional) Enable the function of global isolation forwarding of ARP guard.

arp-guard isolate-forwarding enable

The function of global isolation forwarding of ARP guard is enabled by default.

(7) (Optional) Enable the function of port-based rate limit forwarding of ARP guard.

arp-guard ratelimit-forwarding enable

The function of port-based rate limit forwarding of ARP guard is disabled by default.

(8) Configure the monitoring time of ARP guard.

arp-guard monitor-period *interval*

The default monitoring time of ARP guard is **600** seconds.

(9) Configure the maximum number of monitored hosts of ARP guard in global configuration mode.

arp-guard monitored-host-limit *limit-number*

The maximum number of monitored hosts of ARP guard in global configuration mode is **20000** by default.

(10) Configure a global rate limiting threshold of ARP guard.

arp-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* | **per-src-mac** *rate-limit* }

By default, the global rate limiting threshold of ARP guard for each interface is 128 packets per second, for each source IP address is 30 packets per second, and for each source MAC address is 30 packets per second.

(11) Configure a global attack threshold of ARP guard.

arp-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* | **per-src-mac** *attack-threshold* }

By default, the global attack threshold of ARP guard for each interface is 200 packets per second, for each source IP address is 100 packets per second, and for each source MAC address is 100 packets per second.

(12) Configure a global scanning threshold of ARP guard.

arp-guard scan-threshold *scan-threshold*

By default, the global scanning threshold of ARP guard is 100 packets every 10 seconds.

1.3.4 Procedure (Interface Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4) Enable the ARP guard function on an interface.

nfpp arp-guard enable

The ARP guard function is disabled on an interface by default.

(5) Configure the isolation time of ARP guard on an interface.

nfpp arp-guard isolate-period [*interval* | **permanent**]

No isolation time of ARP guard is configured on an interface by default. The global isolation time of ARP guard is used.

(6) Configure a rate limiting threshold and an attack threshold of ARP guard on an interface.

nfpp arp-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

No local rate limiting threshold or local attack threshold of ARP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of ARP guard are used.

(7) Configure a local scanning threshold of ARP guard on an interface.

nfpp arp-guard scan-threshold *scan-threshold*

No local scanning threshold of ARP guard is configured on an interface by default. The global scanning threshold of ARP guard is used.

1.4 Configuring IP Guard

1.4.1 Overview

After the IP guard function is enabled, a device can detect several common types of IP attacks timely, and ensure its stable operation by rate limit and host isolation. IP guard includes the following functions:

- Identify IP attacks based on hosts or physical ports. This function can determine an attack host based on the source IP address, VLAN ID, and physical port. A rate limiting threshold and an attack threshold can be configured for each attack identification method. When the IP packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the IP packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent to remind users of IP attacks.
- Identify IP scanning attacks. For the IP packets received within 10 seconds, if the source IP address is unchanged and the destination IP address (not the local address) is changing more than the specified scanning threshold of times, an IP scanning attack is suspected and an alarm is printed to remind users.
- Isolate IP attackers based on hosts. This function configures hardware entries to isolate identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
- Monitor attack hosts through software.
  - After this function identifies any attacks, it can monitor the attack host through software in the configured monitoring time.
  - This function can configure a specified host as a trusted host based on its IP address so that the host is free from software monitoring and allowed to send packets to the CPU.

1.4.2 Restrictions and Guidelines

- IP guard is to solve IP attacks whose destination IP address is not a local IP address. If the destination IP address is a local IP address, the rates of IP packets are limited by the function of CPU protect policy (CPP).
- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails. For example, if the IP guard function is enabled on an interface and then disabled in global configuration mode, the function is still enabled on this interface.
- After the IP guard function is disabled, the system automatically clears the entries related to the monitored hosts.
- The rate limiting threshold configured based on a source IP address has a higher priority than that configured based on a port.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure isolation time to discard the packets and prevent them from occupying bandwidth. When you configure isolation time, you must note that:

- If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
- If you change the isolation time to 0 from a non-zero value, entries related to the isolated attacker are directly deleted without monitoring the attacker through software.

- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.
- IP guard can be configured with trusted hosts. When entries in the table of monitored hosts match the trusted hosts (their IP addresses are the same), the system automatically deletes the entries of the IP addresses. IP guard can be configured with a maximum of 500 trusted hosts.

1.4.3 Procedure (Global Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the NFPP configuration mode.

nfpp

(4) Enable the global IP guard function.

ip-guard enable

The global IP guard function is enabled by default.

(5) (Optional) Configure the global isolation time of IP guard.

ip-guard isolate-period [*interval* | **permanent**]

The default global isolation time of IP guard is **0**, and the isolation function is disabled by default.

If the isolation function is enabled, attack host information occupies a hardware entry of the security module.

(6) Configure the monitoring time of IP guard.

ip-guard monitor-period *interval*

The default monitoring time of IP guard is **600** seconds.

(7) Configure the maximum number of monitored hosts of IP guard.

ip-guard monitored-host-limit *number*

The maximum number of monitored hosts of IP guard is **20000** by default.

(8) (Optional) Configure a global rate limiting threshold of IP guard.

ip-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* }

By default, the global rate limiting threshold of IP guard for each interface is 50 packets per second, and for each source IP address is 20 packets per second.

(9) Configure a global attack threshold of IP guard.

ip-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* }

By default, the global attack threshold of IP guard for each interface is 200 packets per second, and for each source IP address is 100 packets per second.

(10) Configure a global scanning threshold of IP guard.

ip-guard scan-threshold *scan-threshold*

By default, the global scanning threshold of IP guard is 100 packets every 10 seconds.

(11) (Optional) Configure the trusted hosts of IP guard.

ip-guard trusted-host *ipv4-address mask*

No host is configured as a trusted host of IP guard by default.

1.4.4 Procedure (Interface Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4) Enable the IP guard function on an interface.

nfpp ip-guard enable

The IP guard function is disabled on an interface by default.

(5) Configure the local isolation time of IP guard on an interface.

nfpp ip-guard isolate-period [*interval* | **permanent**]

No isolation time of IP guard is configured by default.

(6) Configure a local rate limiting threshold and a local attack threshold of IP guard on an interface.

nfpp ip-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* }

No local rate limiting threshold or local attack threshold of IP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of IP guard are used.

(7) Configure a scanning threshold of IP guard on an interface.

nfpp ip-guard scan-threshold *scan-threshold*

No local scanning threshold of IP guard is configured on an interface by default. The global scanning threshold of IP guard is used.

1.5 Configuring TCP-SYN Guard

1.5.1 Overview

An attacker can launch an attack against the device connected through TCP connections. To detect and prevent the TCP-SYN flooding attacks, you can enable the TCP-SYN guard function on the devices. TCP-SYN guard includes the following functions:

- Identify TCP-SYN attacks based on hosts or physical ports. This function can determine an attack host based on the source IP address, VLAN ID, and physical port. A rate limiting threshold and an attack threshold can be configured for each attack identification method. When the TCP-SYN packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the TCP-SYN packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent.
- Isolate TCP-SYN attackers based on hosts. This function configures hardware entries to isolate identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
- Monitor attack hosts through software.
  - After this function identifies any attacks, it can monitor the attack host through software in the configured monitoring time.
  - This function can configure a specified host as a trusted host of TCP-SYN guard based on its IP address so that it is free from software monitoring and allowed to send packets to the CPU.

1.5.2 Restrictions and Guidelines

- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails.
- The rate limiting threshold configured based on a source IP address has a higher priority than that configured based on a port.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure isolation time to discard the packets and prevent them from occupying bandwidth. When you configure isolation time, you must note that:
  - If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
  - If you change the isolation time to 0 from a non-zero value, entries related to the isolated attacker are directly deleted without monitoring the attacker through software.
- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.

- TCP-SYN guard can be configured with trusted hosts. When entries in the table of monitored hosts match the trusted hosts (their IP addresses are the same), the system automatically deletes the entries of the IP addresses. TCP-SYN guard can be configured with a maximum of 500 trusted hosts.

1.5.3 Procedure (Global Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the NFPP configuration mode.

nfpp

(4) Enable the global TCP-SYN guard function.

tcp-syn-guard enable

The TCP-SYN guard function is disabled on the interface and enabled globally by default.

(5) (Optional) Configure the global isolation time of TCP-SYN guard.

tcp-syn-guard isolate-period [*interval* | **permanent**]

The default global isolation time of TCP-SYN guard is **0**, and the isolation function is disabled by default.

(6) Configure the monitoring time of TCP-SYN guard.

tcp-syn-guard monitor-period *interval*

The default monitoring time of TCP-SYN guard is **600** seconds.

(7) Configure the maximum number of monitored hosts of TCP-SYN guard.

tcp-syn-guard monitored-host-limit *number*

The maximum number of monitored hosts of TCP-SYN guard is **20000** by default.

(8) Configure a global rate limiting threshold of TCP-SYN guard.

tcp-syn-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* }

By default, the global rate limiting threshold of TCP-SYN guard for each interface is 50 packets per second, and for each source IP address is 20 packets per second.

(9) Configure a global attack threshold of TCP-SYN guard.

tcp-syn-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* }

By default, the global attack threshold of TCP-SYN guard for each interface is 200 packets per second, and for each source IP address is 100 packets per second.

(10) (Optional) Configure the trusted hosts of TCP-SYN guard.

tcp-syn-guard trusted-host *ipv4-address mask*

No host is configured as a trusted host of TCP-SYN guard by default.

1.5.4 Procedure (Interface Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4) Enable the TCP-SYN guard function on an interface.

nfpp tcp-syn-guard enable

The TCP-SYN guard function is not configured on an interface by default. The global TCP-SYN guard function is used.

(5) Configure the isolation time of TCP-SYN guard on an interface.

nfpp tcp-syn-guard isolate-period { *interval* | **permanent** }

No local isolation time of TCP-SYN guard is configured by default. The global isolation time of TCP-SYN guard is used.

(6) Configure the local rate limiting threshold and local attack threshold of TCP-SYN guard on an interface.

nfpp tcp-syn-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* }

No local rate limiting threshold or local attack threshold of TCP-SYN guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of TCP-SYN guard are used.

1.6 Configuring ICMP Guard

1.6.1 Overview

The ICMP guard function configured for a device is used to prevent an attacker from consuming system resources by sending many ICMP requests. ICMP guard includes the following functions:

- Identify ICMP attacks based on hosts or physical ports. This function can determine an attack host based on the source IP address, VLAN ID, and port. A rate limiting threshold and an attack threshold can be configured for each attack identification method. When the ICMP packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the ICMP packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent.
- Isolate ICMP attackers based on hosts. This function configures hardware entries to isolate identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
- Monitor attack hosts through software.
  - After this function identifies any attacks, it can monitor the attack host through software in the configured monitoring time.
  - This function can configure a specified host as a trusted host of ICMP guard based on its IP address so that it is free from software monitoring and allowed to send packets to the CPU.

1.6.2 Restrictions and Guidelines

- If this function is configured in global configuration mode and interface configuration mode, the interface

configuration prevails.

- After the ICMP guard function is disabled, the system automatically clears the entries related to the monitored hosts.
- The rate limiting threshold configured based on a source IP address has a higher priority than that configured based on a port.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure isolation time to discard the packets and prevent them from occupying bandwidth. When you configure isolation time, you must note that:
  - If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
  - If you change the isolation time to 0 from a non-zero value, entries related to the isolated attacker are directly deleted without monitoring the attacker through software.
- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.
- ICMP guard can be configured with trusted hosts. When entries in the table of monitored hosts match the trusted hosts (their IP addresses are the same), the system automatically deletes the entries of the IP addresses. ICMP guard can be configured with a maximum of 500 trusted hosts.

1.6.3 Procedure (Global Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the NFPP configuration mode.

nfpp

(4) Enable the function of global ICMP guard.

icmp-guard enable

The function of global ICMP guard is enabled by default.

(5) (Optional) Configure the global isolation time of ICMP guard.

icmp-guard isolate-period [*interval* | **permanent**]

The default global isolation time of ICMP guard is **0**, and the isolation function is disabled by default.

(6) Configure the monitoring time of ICMP guard.

icmp-guard monitor-period *interval*

The default monitoring time of ICMP guard is **600** seconds.

(7) Configure the maximum number of monitored hosts.

icmp-guard monitored-host-limit *number*

The maximum number of monitored hosts is **20000** by default.

(8) Configure the global rate limiting threshold of ICMP guard.

icmp-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* }

By default, the global rate limiting threshold of ICMP guard for each interface is 250 packets per second, and for each source IP address is 200 packets per second.

(9) Configure the global attack threshold of ICMP guard.

icmp-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* }

By default, the global attack threshold of ICMP guard for each interface is 400 packets per second, and for each source IP address is 300 packets per second.

(10) (Optional) Configure the trusted hosts of ICMP guard.

icmp-guard trusted-host *ipv4-address mask*

No host is configured as a trusted host by default.

1.6.4 Procedure (Interface Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4) Enable the ICMP guard function on an interface.

nfpp icmp-guard enable

The ICMP guard function is not configured on an interface by default. The global ICMP guard function is used.

(5) Configure the local isolation time of ICMP guard on an interface.

nfpp icmp-guard isolate-period { *interval* | **permanent** }

No local isolation time of ICMP guard is configured on an interface by default. The global isolation time of ICMP guard is used.

(6) Configure the local rate limiting threshold and local attack threshold of ICMP guard on an interface.

nfpp icmp-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* }

No local rate limiting threshold or local attack threshold of ICMP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of ICMP guard are used.

1.7 Configuring DHCP Guard

1.7.1 Overview

In a DHCP starvation attack, all IP addresses of a DHCP server are exhausted. As a result, the DHCP server fails to provide the address assignment service, thus affecting the network access of legal users. To address this type of attacks, you must deploy the DHCP guard function on a device.

DHCP guard includes the following functions:

- Identify DHCP attacks based on hosts or physical ports. This function can determine an attack host based on the source MAC address, VLAN ID, and port on the link layer. A rate limiting threshold and an attack threshold can be configured for each attack identification method. When the DHCP packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the DHCP packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent.
- Isolate DHCP attackers based on hosts. This function configures hardware entries to isolate identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
- Monitor attack hosts through software. After an attack is identified, this function monitors the attack host through software in the configured monitoring time.

1.7.2 Restrictions and Guidelines

- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails.
- After the DHCP guard function is disabled, the system automatically clears the entries related to the monitored hosts.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure isolation time to discard the packets and prevent them from occupying bandwidth. When you configure isolation time, you must note that:
  - If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
  - If you change the isolation time to 0 from a non-zero value, entries related to the isolated attacker are directly deleted without monitoring the attacker through software.
- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must

manually clear some monitored hosts.

- If a port is configured as trusted by the DHCP Snooping function, the DHCP guard function becomes invalid to avoid misjudging DHCP traffic on the trusted port. For trusted port configuration in DHCP Snooping, see "Configuring DHCP Snooping".

1.7.3 Procedure (Global Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the NFPP configuration mode.

nfpp

(4) Enable the function of global DHCP guard.

dhcp-guard enable

The function of global DHCP guard is enabled by default.

(5) (Optional) Configure the global isolation time of DHCP guard.

dhcp-guard isolate-period { *interval* | **permanent** }

The default global isolation time of DHCP guard is **0**, and the isolation function is disabled by default.

(6) Configure the monitoring time of DHCP guard.

dhcp-guard monitor-period *interval*

The default monitoring time of DHCP guard is **600** seconds.

(7) Configure the maximum number of monitored hosts.

dhcp-guard monitored-host-limit *number*

The maximum number of monitored hosts of DHCP guard is **20000** by default.

(8) Configure the global rate limiting threshold of DHCP guard.

dhcp-guard rate-limit { **per-port** *rate-limit* | **per-src-mac** *rate-limit* }

By default, the global rate limiting threshold of DHCP guard for each interface is 150 packets per second, and for each source IP address is 5 packets per second.

(9) Configure the global attack threshold of DHCP guard.

dhcp-guard attack-threshold { **per-port** *attack-threshold* | **per-src-mac** *attack-threshold* }

By default, the global attack threshold of DHCP guard for each interface is 256 packets per second, and for each source IP address is 10 packets per second.

1.7.4 Procedure (Interface Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4) Enable the DHCP guard function on an interface.

nfpp dhcp-guard enable

The DHCP guard function is disabled on an interface by default. The global DHCP guard function is enabled.

(5) Configure isolation time of DHCP guard on an interface.

nfpp dhcp-guard isolate-period [*interval* | **permanent**]

No local isolation time of DHCP guard is configured on an interface by default. The global isolation time of DHCP guard is used.

(6) Configure the local rate limiting threshold and local attack threshold of DHCP guard on an interface.

nfpp dhcp-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

No local rate limiting threshold or local attack threshold of DHCP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of DHCP guard are used.

1.8 Configuring DHCPv6 Guard

1.8.1 Overview

Like DHCPv4, DHCPv6 has security problems. Therefore, the attack methods of DHCPv4 are applicable to DHCPv6. To prevent this type of attacks, we must also deploy the DHCPv6 guard policy. DHCPv6 guard includes the following functions:

- Identify DHCPv6 attacks based on hosts or physical ports. This function can determine an attack host based on the source MAC address, VLAN ID, and port on the link layer. A rate limiting threshold and an attack threshold can be configured for each attack identification method.
- Isolate DHCPv6 attackers based on hosts. This function configures hardware entries to isolate identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
- Monitor attack hosts through software. After an attack is identified, this function monitors the attack host through software in the configured monitoring time.

1.8.2 Restrictions and Guidelines

- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails.
- After the DHCPv6 guard function is disabled, the system automatically clears the entries related to the monitored hosts.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure isolation time to discard the packets and prevent them from occupying bandwidth. When you configure

isolation time, you must note that:

- If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
- If you change the isolation time to 0 from a non-zero value, entries related to the isolated attacker are directly deleted without monitoring the attacker through software.

- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.
- If a port is configured as trusted by the DHCPv6 Snooping function, the DHCPv6 guard function becomes invalid to avoid misjudging DHCPv6 traffic on the trusted port. For trusted port configuration in DHCPv6 Snooping, see "Configuring DHCPv6 Snooping".

1.8.3 Procedure (Global Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the NFPP configuration mode.

nfpp

(4) Enable the function of global DHCPv6 guard.

dhcpv6-guard enable

The function of global DHCPv6 guard is enabled by default.

(5) Configure the monitoring time of DHCPv6 guard.

dhcpv6-guard monitor-period *interval*

The default monitoring time of DHCPv6 guard is **600** seconds.

(6) Configure the maximum number of monitored hosts.

dhcpv6-guard monitored-host-limit *number*

The maximum number of monitored hosts of DHCPv6 guard is **20000** by default.

(7) Configure the global rate limiting threshold of DHCPv6 guard.

dhcpv6-guard rate-limit { **per-port** *rate-limit* | **per-src-mac** *rate-limit* }

By default, the global rate limiting threshold of DHCPv6 guard for each interface is 150 packets per second, and for each source IP address is 5 packets per second.

(8) Configure the global attack threshold of DHCPv6 guard.

dhcpv6-guard attack-threshold { **per-port** *attack-threshold* | **per-src-mac** *attack-threshold* }

By default, the global attack threshold of DHCPv6 guard for each interface is 256 packets per second, and for each source IP address is 10 packets per second.

1.8.4 Procedure (Interface Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4) Enable the DHCPv6 guard function on an interface.

nfpp dhcpv6-guard enable

The DHCPv6 guard function is disabled on an interface by default. The global DHCPv6 guard function is used.

(5) Configure the local rate limiting threshold and local attack threshold of DHCPv6 guard on an interface.

nfpp dhcpv6-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

No local rate limiting threshold is local attack threshold of DHCPv6 guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of DHCPv6 guard are used.

1.9 Configuring ND Guard

1.9.1 Overview

ND packets of ND guard fall into three types by use:

- Type 1: Neighbor requests and neighbor advertisements, which are used to parse addresses.
- Type 2: Route requests, which are used to discover gateways for hosts.
- Type 3: Route advertisements, which are used to advertise gateways and prefixes; and redirection packets, which are used to advertise better next hops.

ND guard identifies ND packets based on physical ports. This function prevents attacks by configuring rate limiting thresholds for attack ports and isolating the ports.

1.9.2 Restrictions and Guidelines

- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- After you enable the ND Snooping function by running the **ipv6 nd snooping enable** command, all ND packets are NDSNP packets. In this case, you must configure rate limiting thresholds and attack thresholds

for the NDSNP packets to validate the guard.

- After you enable the isolation function, the recorded attack host occupies the security module entry. If the port-based isolation entries take effect, the default action is to discard all attack packets. After you enable the function of port-based rate limit forwarding, you can allow some of packets to pass through by changing the isolation action.
- Rate limit by hardware is ineffective to NDSNP packets.

1.9.3 Procedure (Global Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the NFPP configuration mode.

nfpp

(4) Enable the global ND guard function.

nd-guard enable

The function of global ND guard is enabled by default.

(5) Enable the function of port-based rate limit forwarding of ND guard.

nd-guard ratelimit-forwarding enable

The function of port-based rate limit forwarding of ND guard is enabled by default.

(6) Configure the global rate limiting threshold of ND guard.

nd-guard rate-limit per-port { **ndsnp** *rate-limit* | **ns-na** *rate-limit* | **ra-redirect** *rate-limit* | **rs** *rate-limit* }

By default, the global rate limiting threshold of ND guard for NDSNP packet is 100 packets per second, for neighbor request and neighbor advertisement is 50 packets per second, for route advertisement and redirection is 25 packets per second, and for route request is 25 packets per second.

(7) Configure the global attack threshold of ND guard.

nd-guard attack-threshold per-port { **ndsnp** *attack-threshold* | **ns-na** *attack-threshold* | **ra-redirect** *attack-threshold* | **rs** *attack-threshold* }

By default, the global attack threshold of ND guard for NDSNP packet is 200 packets per second, for neighbor request and neighbor advertisement is 100 packets per second, for route advertisement and redirection is 50 packets per second, and for route request is 50 packets per second.

1.9.4 Procedure (Interface Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4) Enable the ND guard function on an interface.

nfpp nd-guard enable

The ND guard function is disabled on an interface by default. The global ND guard function is enabled.

(5) Configure the local rate limiting threshold and local attack threshold of ND guard on an interface.

nfpp nd-guard policy per-port { **ndsnp** *rate-limit attack-threshold* | **ns-na** *rate-limit attack-threshold* | **ra-redirect** *rate-limit attack-threshold* | **rs** *rate-limit attack-threshold* }

No local rate limiting threshold or local attack threshold of ND guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of ND guard are used.

1.10 Customizing Guard

1.10.1 Overview

Users can customize guard types and guard policies to solve network attacks in special application scenarios.

Customized guard includes the following functions:

- Allow users to combine packet type fields and use them as packet types of customized guard to meet requirements of guard scenarios.
- Configure guard policies based on hosts and ports. Host guard policies include those based on the source IP address, VLAN ID and port, or those based on the source MAC address, VLAN ID and port on the link layer. A rate limiting threshold and an attack threshold can be configured for each guard policy. When the packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent.
- Monitor attack hosts through software.
  - After this function identifies any attacks, it can monitor the attack host through software in the configured monitoring time.
  - This function can configure a specified host as a trusted host based on its IPv4, IPv6, or MAC address so that it is free from software monitoring and allowed to send packets to the CPU without rate limit and processing.

1.10.2 Restrictions and Guidelines

- Customized guard allows users to combine packet type fields to include most existing protocol types and expand new protocol types. Improper configuration of the packet type fields may cause a network exception. Therefore, users must well understand network protocols before they configure this function.
- Customized guard has a higher packet detection priority than basic guard types. When packets match the customized guard policy and the policy of a basic guard type, they preferentially undergo rate limit and attack identification according to the customized guard policy. To ensure the configuration effect of basic guard types, try to refer to the configuration guide when you configure the packet type fields of customized guard.
- Customized guard policies must be configured with different type names and packet types. Matched packet

types must differ from the packet types of existing guard types, including those of basic guard types such as ARP guard, IP guard, ICMP guard, TCP-SYN guard, DHCP guard, DHCPv6 guard, and ND guard.

- You can configure packet types of customized guard by combining the following fields. These fields include Ethernet link layer type (etype), source MAC address (src-mac), destination MAC address (dst-mac), IPv4 or IPv6 protocol number (protocol), source IPv4 or IPv6 address (src-ip/src-ipv6), destination IPv4 or IPv6 address (dst-ip/dst-ipv6), source port on the transport layer (src-port), and destination port on the transport layer (dst-port).

  To configure the matched fields of packet fields, conform with the following limit rules. Otherwise, the configuration fails:

  - The IPv4 or IPv6 protocol number (protocol) is configurable only when the Ethernet link layer type (etype) is IPv4 or IPv6.
  - The source IPv4 address (src-ip) and destination IPv4 address (dst-ip) are configurable only when the Ethernet link layer type (etype) is IPv4.
  - The source IPv6 address (src-ipv6) and destination IPv6 address (dst-ipv6) are configurable only when the Ethernet link layer type (etype) is IPv6.
  - The source port on the transport layer (src-port) and destination port on the transport layer (dst-port) are configurable only when the IPv4 or IPv6 protocol number (protocol) is TCP or UDP.
- For the three types of customized guard policies that are based on the source IP address, source MAC address, and port, you must configure at least one type. That is, you must configure the global rate limiting threshold and global attack threshold of customized guard. Otherwise, the customized guard function does not take effect. You can configure a host policy based on the source IP address, VLAN ID, and port only when the specified Ethernet link layer type (etype) is IPv4 or IPv6.
- The rate limiting threshold based on a source MAC address has a higher priority than that based on a source IP address. The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- Only after you configure packet types and guard policies can you enable the customized guard function. If you do not complete any configuration, you are reminded that the current customized guard is not completely configured and the configuration fails.
- The host policy of customized guard on an interface must be consistent with the global host policy configuration. For example, if no global rate limiting threshold and global attack threshold are configured based on the source IP address, you cannot configure the local rate limiting threshold and local attack threshold on an interface.
- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails.
- After the customized guard function is disabled, the system automatically clears the entries related to the monitored hosts.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.

- When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.

- When you configure trusted hosts, note that:
  - You must configure matched packet types before you configure trusted hosts.
  - The trusted hosts of customized guard must be consistent with the matched packet types. For example, only when the Ethernet link layer type (etype) is IPv4, can you add IPv4 addresses as trusted IP addresses. Similarly, when the matched packet type is IPv4, IPv6 addresses cannot be added as trusted IP addresses.
  - You can configure all hosts in a network segment as trusted hosts by configuring masks.
  - When entries in the table of monitored hosts match the trusted hosts, the system automatically deletes the entries of the IP addresses.
  - ICMP guard can be configured with a maximum of 500 trusted hosts.

1.10.3 Procedure (Global Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the NFPP configuration mode.

nfpp

(4) Customize a guard type, and enter the configuration mode of the NFPP customized guard type.

define *define-name*

(5) Configure the matched packet types of the customized guard type.

match { **dst-ip** *destination-ipv4-address* [**dst-ip-mask** *mask*] | **dst-ipv6** *destination-ipv6-address* [**dst-ipv6-masklen** *prefix-length*] | **dst-mac** *destination-mac* [**dst-mac-mask** *destination-mac-mask*] | **dst-port** *port-number* | **etype** *type* | **protocol** *protocol* | **src-ip** *source-ipv4-address* [**src-ip-mask** *mask*] | **src-ipv6** *source-ipv6-address* [**src-ipv6-masklen** *prefix-length*] | **src-mac** *source-mac-address* | **src-port** *port-number* } *

(6) Configure the global rate limiting threshold and global attack threshold of the customized guard type.

global-policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

No global rate limiting threshold or global attack threshold of the customized guard type is configured by default.

They must be configured. Otherwise, you cannot enable the customized guard function.

(7) Configure the monitoring time of the customized guard type.

monitor-period *interval*

The default monitoring time of a customized guard type is **600** seconds.

(8) Configure the maximum number of monitored hosts of the customized guard type.

monitored-host-limit *number*

The maximum number of monitored hosts is **20000** by default.

(9) Configure the trusted hosts of the customized guard type.

trusted-host { *ipv4-address mask* | *ipv6-address/prefix-length* | *mac-address mask* }

No host is configured as a trusted host of the customized guard type by default.

(10) Enable the function of global customized guard.

define *define-name* **enable**

The function of global customized guard is disabled by default.

1.10.4 Procedure (Interface Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4) Enable the customized guard function on an interface.

nfpp define *define-name* **enable**

The customized guard function is disabled on an interface by default. The global customized guard function is used.

(5) Configure the local rate limiting threshold and local attack threshold of the customized guard type on an interface.

nfpp define *define-name* **policy** { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

No local rate limiting threshold or local attack threshold of the customized guard type is configured on an interface by default. The global rate limiting threshold and global attack threshold of the customized guard type are used.

1.11 Disabling Guard

1.11.1 Overview

Users can disable or enable all basic types of global guard function by running one command. Basic guard types supported by this function include ARP guard, IP guard, ICMP guard, TCP-SYN guard, DHCP guard, DHCPv6 guard, and ND guard.

1.11.2 Restrictions and Guidelines

- This function applies to only basic guard types and does not affect the customized guard types.
- This function applies to the guard functions in global configuration mode and does not affect the guard functions in interface configuration mode.

- After you run the one-click enabling/disabling command, the configuration of this command cannot be displayed by running the **show running-config** command.
- The one-click enabling/disabling command is to actually enable or disable basic guard types in global configuration mode. After you run this command to disable basic guard types, the **show running-config** command allows you to display the global disabling command of each basic guard function. After you run this command to enable basic guard types, the **show running-config** command allows you to display the default configuration.
- This command cannot be saved, but its running result can be saved and take effect after device restart.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable all the basic types of global guard of NFPP.

all-guard enable

1.12 Configuring NFPP Logs

1.12.1 Overview

When many attacks are launched to a device, the generated prompts may affect user experience. You can configure the size of a log buffer, system message rate, and filtering conditions to restrictively record and display logs.

- NFPP retrieves logs from a special buffer at a rate, uses them to generate system messages, and clears the logs from the buffer. Therefore, you can configure the rate of generating system messages from logs of the log buffer through NFPP to control the message report frequency and avoid log spamming.
- You can also configure filtering conditions to obtain required log information accurately and filter out logs that do not comply with the filtering rules.
- To monitor whether an attack occurs, you can print logs on a screen in real time.

1.12.2 Restrictions and Guidelines

- After active/standby switchover of a device, the device will clear logs in a buffer and record new logs again.
- Even if a device does not suffer an attack, logs are continuously retrieved from the buffer to generate system messages.
- When the log buffer overflows, new logs overwrite the stale logs, and the log buffer displays an entry with attributes being "-". In this case, you must increase the log buffer size or improve the generation rate of system messages.

1.12.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the NFPP configuration mode.

nfpp

(4) Configure the size of a log buffer.

log-buffer entries *number*

The default size of the NFPP log buffer is **256** entries.

(5) Configure the rate of generating system messages from logs of the log buffer through NFPP.

log-buffer logs *message-number* **interval** *interval*

No rate of generating system messages from logs of the log buffer is configured through NFPP and NFPP logs are not written into the buffer by default.

If the values of the *message-number* and *interval* parameters are **0**, logs are used by NFPP to immediately generate system messages without being written into the buffer.

(6) Configure NFPP to record the logs of a specified VLAN and a specified interface.

logging { **interface** *interface-type interface-number* | **vlan** *vlan-range* }

NFPP records the logs of all VLANs and interfaces by default.

(7) Enable the function of screen log output.

log-buffer enable

The function of screen log output is disabled by default and logs are saved in the buffer.

1.13 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Notice

- Running the **clear** command may lose vital information and thus interrupt services.

Table 1-1 Monitoring

Command	Purpose
clear nfpp arp-guard scan	Clears the scanning table of ARP guard.
clear nfpp arp-guard hosts	Clears the monitored hosts of ARP guard.
clear nfpp ip-guard hosts	Clears the monitored hosts of IP guard.
clear nfpp tcp-syn-guard hosts	Clears the monitored hosts of TCP-SYN guard.
clear nfpp nd-guard hosts	Clears the monitored hosts of ND guard.
clear nfpp icmp-guard hosts	Clears the monitored hosts of ICMP guard.

Command	Purpose
clear nfpp dhcp-guard hosts	Clears the monitored hosts of DHCP guard.
clear nfpp dhcpv6-guard hosts	Clears the monitored hosts of DHCPv6 guard.
clear nfpp define *define-name* **hosts**	Clears the monitored hosts of customized guard.
clear nfpp log	Clears logs.
show nfpp arp-guard summary	Displays the configuration parameters of ARP guard.
show nfpp arp-guard hosts	Displays the monitored hosts of ARP guard.
show nfpp arp-guard scan	Displays the scanning table of ARP guard.
show nfpp ip-guard summary	Displays the configuration parameters of IP guard.
show nfpp ip-guard hosts	Displays the monitored hosts of IP guard.
show nfpp ip-guard trusted-host	Displays the scanning table of IP guard.
show nfpp tcp-syn-guard summary	Displays the configuration parameters of TCP-SYN guard.
show nfpp tcp-syn-guard hosts	Displays the monitored hosts of TCP-SYN guard.
show nfpp tcp-syn-guard trusted-host	Displays the scanning table of TCP-SYN guard.
show nfpp icmp-guard summary	Displays the configuration parameters of ICMP guard.
show nfpp icmp-guard hosts	Displays the monitored hosts of ICMP guard.
show nfpp icmp-guard trusted-host	Displays the scanning table of ICMP guard.
show nfpp dhcp-guard summary	Displays the configuration parameters of DHCP guard.
show nfpp dhcp-guard hosts	Displays the monitored hosts of DHCP guard.
show nfpp dhcpv6-guard summary	Displays the configuration parameters of DHCPv6 guard.
show nfpp dhcpv6-guard hosts	Displays the monitored hosts of DHCPv6 guard.
show nfpp nd-guard summary	Displays the configuration parameters of ND guard.
show nfpp define summary [*name*]	Displays the configuration parameters of customized guard.
show nfpp define hosts *name*	Displays the monitored hosts.
show nfpp define trusted-host *name*	Displays the trusted hosts.
show nfpp log summary	Displays the configuration of NFPP logs.
show nfpp log buffer [**statistics**]	Displays the log buffer of NFPP.

1.14 Configuration Examples

1.14.1 Configuring CPU Guard

1. Requirements

In a network system, protocols such as ARP, IP, TCP-SYN, ICMP, DHCP, DHCPv6, and ND are popular targets of attacks. This may cause packet forwarding failure and high CPU usage. You can enable guard policies to ensure the stable running of devices.

2. Notes

- Configure the rate limiting threshold, attack threshold and isolation time of ARP guard.
- Configure the scanning threshold and isolation time of IP guard.
- Configure the scanning threshold and isolation time of TCP-SYN guard.
- Configure the scanning threshold and isolation time of ICMP guard.
- Configure the scanning threshold and isolation time of DHCP guard.
- Configure the scanning threshold and isolation time of DHCPv6 guard.
- Configure the scanning threshold and isolation time of ND guard.

3. Procedure

Configure ARP guard on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# nfpp
DeviceA(config-nfpp)# arp-guard rate-limit per-src-mac 5
DeviceA(config-nfpp)# arp-guard attack-threshold per-src-mac 10
DeviceA(config-nfpp)# arp-guard isolate-period 180
```

Configure IP guard on Device A.

```
DeviceA(config-nfpp)# ip-guard rate-limit per-src-ip 20
DeviceA(config-nfpp)# ip-guard attack-threshold per-src-ip 30
DeviceA(config-nfpp)# ip-guard isolate-period 180
DeviceA(config-nfpp)# ip-guard trusted-host 192.168.201.46 255.255.255.255
```

Configure TCP-SYN guard on Device A.

```
DeviceA(config-nfpp)# tcp-syn-guard rate-limit per-src-ip 20
DeviceA(config-nfpp)# tcp-syn-guard attack-threshold per-src-ip 30
DeviceA(config-nfpp)# tcp-syn-guard isolate-period 180
DeviceA(config-nfpp)# tcp-syn-guard trusted-host 192.168.201.46 255.255.255.255
```

Configure ICMP guard on Device A.

```
DeviceA(config-nfpp)# icmp-guard rate-limit per-src-ip 20
DeviceA(config-nfpp)# icmp-guard attack-threshold per-src-ip 30
DeviceA(config-nfpp)# icmp-guard isolate-period 180
```

Configure DHCP guard on Device A.

```
DeviceA(config-nfpp)# dhcp-guard rate-limit per-src-ip 20
```

```
DeviceA(config-nfpp)# dhcp-guard attack-threshold per-src-ip 30
DeviceA(config-nfpp)# dhcp-guard isolate-period 180
DeviceA(config-nfpp)# dhcp-guard trusted-host 192.168.201.46 255.255.255.255
```

Configure DHCPv6 guard on Device A.

```
DeviceA(config-nfpp)# dhcpv6-guard rate-limit per-src-ip 20
DeviceA(config-nfpp)# dhcpv6-guard attack-threshold per-src-ip 30
DeviceA(config-nfpp)# dhcpv6-guard trusted-host 192.168.201.46 255.255.255.255
```

Configure ND guard on Device A.

```
DeviceA (config-nfpp)# nd-guard rate-limit per-port ns-na 30
DeviceA (config-nfpp)# nd-guard attack-threshold per-port ns-na 50
```

4. Verification

Run the **show nfpp arp-guard summary** command to display the configuration.

```
DeviceA# show nfpp arp-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-
port.)
Interface Status  Isolate-period Rate-limit     Attack-threshold Scan-threshold
Global    Disable 180          4/5/100        8/10/200        15

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

Run the **show nfpp arp-guard hosts** command to display the monitored hosts.

```
DeviceA# show nfpp arp-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address       MAC address    remain-time(s)
 ----    ---------   ----------       -----------    --------------
 1      Gi0/43     5.5.5.16        -            175
Total: 1 host
```

Run the **show nfpp arp-guard scan** command to display the scanned hosts.

```
DeviceA# show nfpp arp-guard scan
VLAN  interface      IP address       MAC address    timestamp
----  ---------      ----------       -----------    ---------
1    Gi0/5         -               001a.a9c2.4609  2013-4-30 23:50:32
1    Gi0/5         192.168.206.2    001a.a9c2.4609  2013-4-30 23:50:33
1    Gi0/5         -               001a.a9c2.4609  2013-4-30 23:51:33
1    Gi0/5         192.168.206.2    001a.a9c2.4609  2013-4-30 23:51:34
Total: 4 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp arp-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp ip-guard summary** command to display the configuration.

```
DeviceA# show nfpp ip-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-
port.)
Interface Status  Isolate-period Rate-limit     Attack-threshold Scan-threshold
Global    Disable 180          20/-/100       30/-/200        100

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

Run the **show nfpp ip-guard hosts** command to display the monitored hosts.

```
DeviceA# show nfpp ip-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address       Reason    remain-time(s)
 ----    ---------   ----------       ------    --------------
  1      Gi0/5       192.168.201.47   ATTACK    160
Total: 1 host
```

Run the **show nfpp ip-guard trusted-host** command to display the trusted hosts.

```
DeviceA# show nfpp ip-guard trusted-host
IP address         mask
----------         ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp ip-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp tcp-syn-guard summary** command to display the configuration.

```
DeviceA# show nfpp tcp-syn-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-
port.)
Interface Status  Isolate-period Rate-limit     Attack-threshold Scan-threshold
Global    Disable 180          20/-/100       30/-/200        100

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

Run the **show nfpp tcp-syn-guard hosts** command to display the monitored hosts.

Run the **show nfpp tcp-syn-guard trusted-host** command to display the trusted hosts.

```
DeviceA# show nfpp tcp-syn-guard trusted-host
IP address         mask
----------         ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp tcp-syn-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp icmp-guard summary** command to display the configuration.

```
DeviceA# show nfpp icmp-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status  Isolate-period Rate-limit     Attack-threshold Scan-threshold
Global    Disable 180          20/-/100       30/-/200        100

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

Run the **show nfpp icmp-guard hosts** command to display the monitored hosts.

```
DeviceA# show nfpp icmp-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address       Reason    remain-time(s)
 ----    ---------   ----------       ------    --------------
  1      Gi0/5       192.168.201.47   ATTACK    160
Total: 1 host
```

Run the **show nfpp icmp-guard trusted-host** command to display the trusted hosts.

```
DeviceA# show nfpp icmp-guard trusted-host
IP address         mask
----------         ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp icmp-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp dhcp-guard summary** command to display the configuration.

```
DeviceA# show nfpp dhcp-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status  Isolate-period Rate-limit     Attack-threshold Scan-threshold
Global    Disable 180          20/-/100       30/-/200        100

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

Run the **show nfpp dhcp-guard hosts** command to display the monitored hosts.

```
DeviceA# show nfpp dhcp-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address       Reason    remain-time(s)
 ----    ---------   ----------       ------    --------------
  1      Gi0/5       192.168.201.47   ATTACK    160
Total: 1 host
```

Run the **show nfpp dhcp-guard trusted-host** command to display the trusted hosts.

```
DeviceA# show nfpp dhcp-guard trusted-host
IP address         mask
----------         ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp dhcp-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp dhcpv6-guard summary** command to display the configuration.

```
DeviceA# show nfpp dhcpv6-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-
port.)
Interface Status  Isolate-period Rate-limit     Attack-threshold Scan-threshold
Global    Disable 180           20/-/100       30/-/200         100

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

Run the **show nfpp dhcpv6-guard hosts** command to display the monitored hosts.

```
DeviceA# show nfpp dhcpv6-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address       Reason    remain-time(s)
 ----    ---------   ----------       ------    --------------
  1      Gi0/5       192.168.201.47   ATTACK    160
Total: 1 host
```

Run the **show nfpp dhcpv6-guard trusted-host** command to display the trusted hosts.

```
DeviceA# show nfpp dhcpv6-guard trusted-host
IP address         mask
----------         ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp dhcpv6-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp nd-guard summary** command to display the configuration.

```
DeviceA# show nfpp nd-guard summary
(Format of column Rate-limit and  Attack-threshold is NS-NA/RS/RA-REDIRECT/ND-
SNP.)
Interface Status  Rate-limit      Attack-threshold
Global    Disable 30/25/25/25
```

Contents

1 Configuring Storm Control....1
1.1 Introduction....1
1.1.1 Overview....1
1.1.2 Principles....1
1.2 Configuring Storm Control....1
1.3 Monitoring....2
1.4 Configuration Examples....2

1 Configuring Storm Control

1.1 Introduction

1.1.1 Overview

When a local area network (LAN) has excess broadcast, multicast, or unknown unicast data flows, the network speed will slow down and packet transmission will have an increased timeout probability. This situation is called a LAN storm. A storm may occur when topology protocol execution or network configuration is incorrect.

Storm control can be implemented to limit broadcast, multicast, or unknown unicast data flows. When the rate of broadcast, multicast, or unknown unicast data flows received over a device port exceeds the specified range, the device transmits only packets in the specified range and discards packets beyond the range until the packet rate falls within the range. This prevents flooded data from entering the LAN and causing a storm.

1.1.2 Principles

1. Storm Control Based on the Percentage-based Bandwidth Threshold

If the rate of data flows received over a device port exceeds the specified bandwidth, excess data flows are discarded until the rate falls within the threshold.

Instruction

Due to chip implementation limitations, when the storm suppression threshold is set to the percentage-based bandwidth, the configured value is converted to a multiple of the step supported by the chip. Therefore, the actual effective suppression threshold on a port may be smaller than the configured suppression threshold.

2. Storm Control Based on the Packets-per-Second Threshold

If the rate of data flows received over a device port exceeds the configured packets-per-second threshold, excessive data flows are discarded until the rate falls within the threshold.

3. Storm Control Based on the Kilobits-per-Second Threshold

If the rate of data flows received over a device port exceeds the configured kilobits-per-second threshold, excessive data flows are discarded until the rate falls within the threshold.

Instruction

Due to chip implementation limitations, when the storm suppression threshold is set to kilobits-per-second, the configured value is converted to a multiple of the step supported by the chip. Therefore, the actual effective suppression threshold on a port may be smaller than the configured suppression threshold.

1.2 Configuring Storm Control

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable packet storm control.

storm-control { **broadcast** | **multicast** | **unicast** } [**level** *percent* | **pps** *packets* | *rate*]

Packet storm control is disabled by default.

1.3 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show storm-control [*interface-type interface-number*]	Displays storm control information.

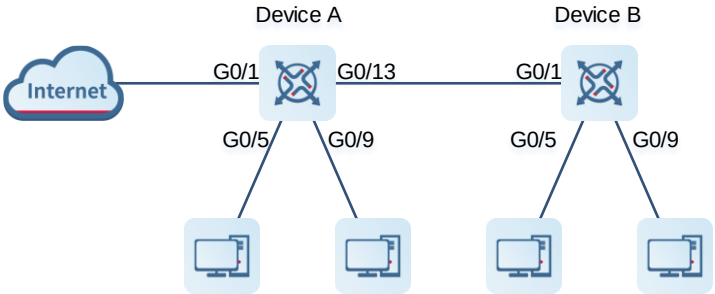
1.4 Configuration Examples

1. Requirements

Enable storm control to prevent excessive broadcast, multicast, or unknown unicast data flows in a LAN, which will cause the network speed to slow down.

2. Topology

Figure 1-1 Topology of Configuring Storm Control



3. Notes

Enable storm control on access devices A and B.

4. Procedure

(1) Enable storm control on Device A.

```
DeviceA> enable
DeviceA# configure terminal
```

```
DeviceA(config)# interface range gigabitethernet 0/5,0/9,0/13
DeviceA(config-if-range)# storm-control broadcast
DeviceA(config-if-range)# storm-control multicast
DeviceA(config-if-range)# storm-control unicast
```

(2) Enable storm control on Device B.

```
DeviceA> enable
DeviceA# configure terminal
DeviceB(config)# interface range gigabitethernet 0/1,0/5,0/9
DeviceB(config-if-range)# storm-control broadcast
DeviceB(config-if-range)# storm-control multicast
DeviceB(config-if-range)# storm-control unicast
```

5. Verification

(1) Check whether storm control is enabled on Device A.

```
DeviceA# show storm-control
Interface              Broadcast Control Multicast Control Unicast Control
Action
------------------------ ---------------- ---------------- ---------------
--------
     GigabitEthernet 0/1        Disabled        Disabled       Disabled
none
     GigabitEthernet 0/5         default         default        default
none
     GigabitEthernet 0/9         default         default        default
none
     GigabitEthernet 0/13        default         default        default
none
```

(2) Check whether storm control is enabled on Device B.

```
DeviceA# show storm-control
Interface              Broadcast Control Multicast Control Unicast Control
Action
------------------------ ---------------- ---------------- ---------------
--------
     GigabitEthernet 0/1         default         default        default
none
     GigabitEthernet 0/5         default         default        default
none
     GigabitEthernet 0/9         default         default        default
none
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/5
```

```
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/9
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/13
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
End
```

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/1
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/5
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/9
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
end
```

Contents

1 Configuring uRPF....1
1.1 Introduction....1
1.1.1 Overview....1
1.1.2 Principles....1
1.1.3 Protocols and Standards....2
1.2 Restrictions and Guidelines....2
1.3 Configuration Task Summary....3
1.4 Enabling Global uRPF....3
1.4.1 Overview....3
1.4.2 Restrictions and Guidelines....3
1.4.3 Procedure....3
1.5 Enabling uRPF on an Interface....3
1.5.1 Overview....3
1.5.2 Restrictions and Guidelines....4
1.5.3 Procedure....4
1.6 Configuring uRPF Packet Loss Rate Advertisement....4
1.6.1 Overview....4
1.6.2 Restrictions and Guidelines....4
1.6.3 Configuration Tasks....4
1.6.4 Configuring Global Packet Loss Rate Parameters....5
1.6.5 Configuring Packet Loss Rate Parameters on an Interface....5
1.7 Monitoring....5

1.8 Configuration Examples.....6

1.8.1 Configuring the uRPF Strict Mode.....6

1.8.2 Configuring the uRPF Loose Mode 9

1 Configuring uRPF

1.1 Introduction

1.1.1 Overview

Unicast Reverse Path Forwarding (uRPF) is a function that protects the network against source address spoofing.

uRPF obtains the source address and inbound interface of a received packet and searches for a forwarding entry in the forwarding table based on the source address. If no entry is configured, the packet is discarded. In uRPF strict mode, if the outbound interface of the forwarding entry does not match the inbound interface of the packet, the packet is also discarded.

1.1.2 Principles

1. Basic Concepts

- uRPF strict mode

  uRPF obtains the source address and inbound interface of a received packet and searches for a forwarding entry in the forwarding table based on the source address. If the entry does not exist, the packet is discarded. If the outbound interface of the forwarding entry does not match the inbound interface of the packet, the packet is also discarded. The strict mode requires that the inbound interface of a received packet must be the outbound interface of the route entry to the source address of the packet.

  The uRPF strict mode is often deployed on a point-to-point (P2P) interface, and inbound and outbound data streams must go through the network of the P2P interface. uRPF blocks the packets with spoofed source addresses at the access layer or aggregation layer to prevent sending such packets from PCs to the core network.

- uRPF loose mode

  uRPF reversely searches for a route based on the source IP address of a received packet. The outbound interface of the next hop on the route does not need to be the inbound interface of the received packet. However, the route cannot be a route of a host on the local network.

  The loose mode is applicable to asymmetric routes or multi-homed networks with asymmetric traffic. On a multi-homed network, the user network is connected to multiple Internet service providers (ISPs), and the inbound and outbound traffic is not symmetric. To prevent invalid packets from attacking the user network, deploy the uRPF loose mode on the outbound interface connected to ISPs.

- uRPF packet loss rate

  The uRPF packet loss rate is the number of packets discarded due to the uRPF check per second. The unit is packets/second, that is, pps.

- Interval for calculating the uRPF packet loss rate

  It refers to the interval from the previous time the packet loss rate is calculated to the current time the packet loss rate is calculated.

- Sampling interval of the uRPF packet loss rate

It refers to the interval at which the number of lost packets is collected for calculating the packet loss rate. This interval must be greater than or equal to the interval for calculating the packet loss rate.

- Threshold of the uRPF packet loss rate

  It refers to the maximum packet loss rate that is acceptable. When the packet loss rate exceeds the threshold, alarms can be sent to users through syslogs or trap messages. You can adjust the threshold of the packet loss rate based on the actual network conditions.

- Alarm interval of the uRPF packet loss rate

  It refers to the interval at which alarms are sent to users. You can adjust the alarm interval based on the actual network conditions to prevent frequent output of logs or trap messages.

2. Enabling uRPF

Enable uRPF to perform a uRPF check on IP packets, thus protecting the device against source address spoofing.

uRPF can be configured in global or interface configuration mode.

Notice

uRPF cannot be configured in global configuration mode and interface configuration mode simultaneously.

- Global configuration mode

  After uRPF is enabled in global configuration mode, a device will perform a uRPF check for packets received over all interfaces of the device.

- Interface configuration mode

  uRPF is performed for packets received on the configured interface.

3. Notifying the uRPF Packet Loss Rate

To conveniently monitor lost packets after uRPF is enabled, the device uses syslogs or trap messages to proactively notify users of the packet loss information detected in the uRPF check.

In the period from the time when uRPF is enabled to the time when the sampling interval arrives, the packet loss rate is the number of lost packets measured within the sampling interval divided by the uRPF enabling time. After that, the packet loss rate is calculated as follows:

Current packet loss rate = (Current number of lost packets measured at the calculation interval – Number of lost packets measured before the sampling interval)/Sampling interval

1.1.3 Protocols and Standards

- RFC 2827: Network Ingress Filtering: DDOS Attacks which employ IP Source Address Spoofing
- RFC 3704: Ingress Filtering for Multi-homed Networks

1.2 Restrictions and Guidelines

- uRPF is implemented with the help of existing unicast routes in the network. Therefore, unicast routes must be configured in the network.
- uRPF checks only source addresses of packets whose destination addresses are unicast addresses and does not check packets whose destination addresses are multicast or IPv4 broadcast addresses.
- uRPF cannot be enabled on a range of interfaces.

- uRPF does not check DHCP/BOOTP packets whose source IP address is 0.0.0.0 and destination IP address is 255.255.255.255.
- uRPF does not check loopback packets sent by the local device to itself.

1.3 Configuration Task Summary

uRPF configuration includes the following tasks:

(1) Enabling uRPF. Please configure only one task.

- Enabling Global uRPF
- Enabling uRPF on an Interface

(2) (Optional) Configuring uRPF Packet Loss Rate Advertisement. Configure at least one of the tasks.

- Configuring Global Packet Loss Rate Parameters
- Configuring Packet Loss Rate Parameters on an Interface

1.4 Enabling Global uRPF

1.4.1 Overview

After global uRPF is enabled, a uRPF check is performed for packets received over all interfaces of a device to protect the device against source address spoofing.

1.4.2 Restrictions and Guidelines

- Only the uRPF strict mode can be configured in global configuration mode. If a matched equal-cost route is found for a packet, the packet will be processed according to the uRPF loose mode.
- If global uRPF is enabled, the default route cannot be used for the uRPF check.
- uRPF cannot be configured in global configuration mode and interface configuration mode simultaneously.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable global uRPF. Configure at least one of the tasks.

- Enable global IPv4 uRPF.

  ip verify unicast source reachable-via rx

  IPv4 uRPF is disabled by default.

1.5 Enabling uRPF on an Interface

1.5.1 Overview

uRPF is performed for packets received on the configured interface to prevent source address spoofing.

1.5.2 Restrictions and Guidelines

- Both the uRPF strict mode and loose mode can be configured on an interface.
- uRPF cannot be configured in global configuration mode and interface configuration mode simultaneously.
- The default route is not used for a uRPF check by default. You can configure **allow-default** to use the default route for a uRPF check if necessary.
- The uRPF strict mode supports matching of equal-cost routes. If a packet received on an interface matches an equal-cost route during the uRPF check, the packet will be processed according to the uRPF loose mode.
- After uRPF is enabled, the route forwarding capacity of a device will be reduced by half.
- After uRPF is enabled on interfaces, a uRPF check is performed for all packets received on physical ports corresponding to these interfaces, which increases the scope of packets checked by uRPF. If a packet received on a tunnel port is also received on the preceding physical ports, the packet is also checked by uRPF. In such a scenario, be cautious in enabling uRPF.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable uRPF for an interface. Configure at least one of the tasks.

- Enable IPv4 uRPF for an interface.

  ip verify unicast source reachable-via { **any** | **rx** } [**allow-default**]

  IPv4 uRPF is disabled for an interface by default.

  support configuration of IPv4 uRPF on a routed port or L3 AP port.

1.6 Configuring uRPF Packet Loss Rate Advertisement

1.6.1 Overview

After uRPF packet loss information monitoring is enabled, a device can proactively send syslogs or trap messages to notify users of the packet loss information detected in the uRPF check so that the users can monitor the network status conveniently.

1.6.2 Restrictions and Guidelines

uRPF must be enabled.

1.6.3 Configuration Tasks

Configure at least one of the tasks.

- Configuring Global Packet Loss Rate Parameters
- Configuring Packet Loss Rate Parameters on an Interface

1.6.4 Configuring Global Packet Loss Rate Parameters

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure global packet loss rate parameters. Configure at least one of the tasks.

- Configure the interval of calculating the uRPF IPv4 packet loss rate.

  ip verify urpf drop-rate compute interval *interval*

  The default interval for calculating the uRPF IPv4 packet loss rate is **30** seconds.

- Configure the alarm interval for the uRPF IPv4 packet loss rate.

  ip verify urpf drop-rate notify hold-down *hold-down-time*

  The default alarm interval for the uRPF IPv4 packet loss rate is **300** seconds.

1.6.5 Configuring Packet Loss Rate Parameters on an Interface

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure packet loss rate parameters on an interface. Configure at least one of the tasks.

- Enable uRPF packet loss information monitoring.

  ip verify urpf drop-rate notify

  uRPF packet loss information monitoring is disabled by default.

- Configure the threshold of the uRPF packet loss rate.

  ip verify urpf notification threshold *rate-value*

  The default threshold of the uRPF packet loss rate is **1000** packets per second.

  If the threshold is **0**, a notification is sent for every packet that is discarded because it fails in the uRPF check.

1.7 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Run the **debug** commands to output debugging information.

Notice

- Running the **clear** command during operation of the device may lose vital information and interrupt services.

- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
show ip urpf [**interface** *interface-type interface-number*]	Displays the IPv4 uRPF configurations and statistics.
clear ip urpf [**interface** *interface-type interface-number*]	Clears IPv4 uRPF packet loss statistics.
debug urpf event	Debugs uRPF events.
debug urpf timer	Debugs uRPF timers.

1.8 Configuration Examples

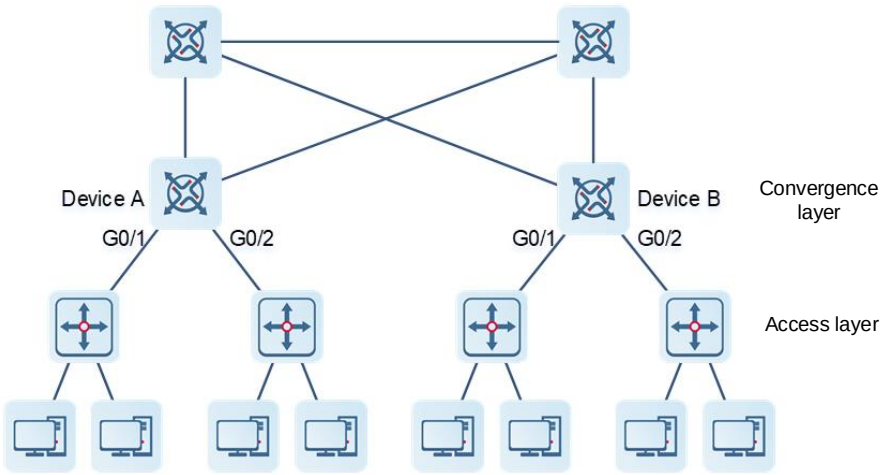
1.8.1 Configuring the uRPF Strict Mode

1. Requirements

In uRPF strict mode, packets with spoofed source addresses are blocked at the access layer or aggregation layer to prevent sending such packets from PCs to the core network.

2. Topology

Figure 1-1 Configuring the uRPF Strict Mode



3. Notes

Enable the uRPF strict mode on the aggregation devices, including Devices A and B.

4. Procedure

(1) Configure Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 195.52.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# ip verify unicast source reachable-via
rx
DeviceA(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet0/2
DeviceA(config-if-GigabitEthernet 0/2)# ip address 195.52.2.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/2)# ip verify unicast source reachable-via
rx
DeviceA(config-if-GigabitEthernet 0/2)# ip verify urpf drop-rate notify
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

(2) Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 195.52.3.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# ip verify unicast source reachable-via
rx
DeviceB(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify
DeviceB(config-if-GigabitEthernet 0/1)# exit
DeviceB(config)# interface gigabitethernet0/2
DeviceB(config-if-GigabitEthernet 0/2)# ip address 195.52.4.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/2)# ip verify unicast source reachable-via
rx
DeviceB(config-if-GigabitEthernet 0/2)# ip verify urpf drop-rate notify
DeviceB(config-if-GigabitEthernet 0/2)# exit
```

5. Verification

If source address spoofing exists on the network, run the **show ip urpf** command to display the number of spoofing packets discarded by uRPF.

Display the number of spoofing packets discarded by uRPF on GigabitEthernet 0/1 of Device A.

```
DeviceA# show ip urpf interface gigabitethernet 0/1
IP verify source reachable-via RX
IP verify URPF drop-rate notify is enabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface is 0
```

Display the number of spoofing packets discarded by uRPF on GigabitEthernet 0/2 of Device A.

```
DeviceA# show ip urpf interface gigabitethernet 0/2
```

```
IP verify source reachable-via RX
IP verify URPF drop-rate notify is enabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 133
Number of drop-rate notification counts in this interface is 0
```

Display the number of spoofing packets discarded by uRPF on GigabitEthernet 0/1 of Device B.

```
DeviceB# show ip urpf interface gigabitethernet 0/1
IP verify source reachable-via RX
IP verify URPF drop-rate notify is enabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface is 0
```

Display the number of spoofing packets discarded by uRPF on GigabitEthernet 0/2 of Device B.

```
DeviceB# show ip urpf interface gigabitethernet 0/2
IP verify source reachable-via RX
IP verify URPF drop-rate notify is enabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 250
Number of drop-rate notification counts in this interface is 0
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 ip address 195.52.1.1 255.255.255.0
 ip verify unicast source reachable-via rx
 ip verify urpf drop-rate notify
!
interface GigabitEthernet 0/2
 ip address 195.52.2.1 255.255.255.0
 ip verify unicast source reachable-via rx
 ip verify urpf drop-rate notify
!
end
```

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/1
 ip address 195.52.3.1 255.255.255.0
 ip verify unicast source reachable-via rx
 ip verify urpf drop-rate notify
!
interface GigabitEthernet 0/2
```

```
 ip address 195.52.4.1 255.255.255.0
 ip verify unicast source reachable-via rx
 ip verify urpf drop-rate notify
!
end
```

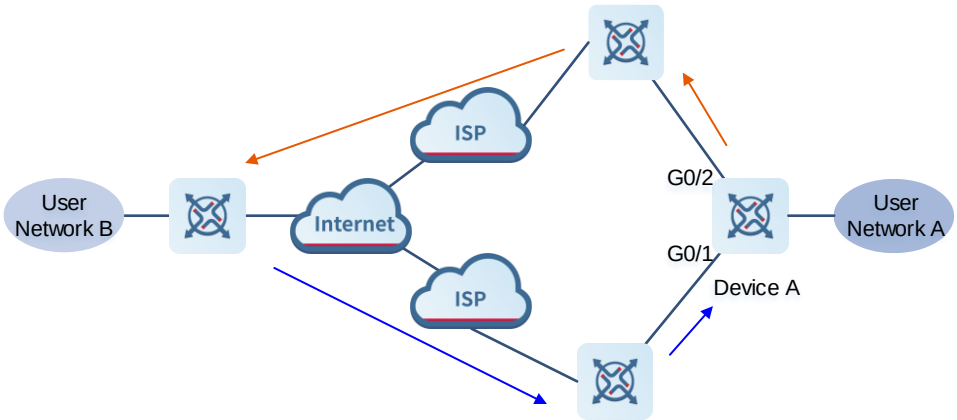
1.8.2 Configuring the uRPF Loose Mode

1. Requirements

To prevent invalid packets from attacking the user network, deploy the uRPF loose mode.

2. Topology

Figure 1-2 Configuring the uRPF Loose Mode



3. Notes

Configure the uRPF loose mode on the outbound interfaces connected to ISPs.

4. Procedure

Enable the uRPF loose mode on GigabitEthernet 0/1 and GigabitEthernet 0/2.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet0/1
DeviceA(config-if-GigabitEthernet0/1)# ip address 195.52.1.2 255.255.255.252
DeviceA(config-if-GigabitEthernet0/1)# ip verify unicast source reachable-via any
DeviceA(config-if-GigabitEthernet0/1)# ip verify urpf drop-rate notify
DeviceA(config-if-GigabitEthernet0/1)# exit
DeviceA(config)# interface gigabitethernet0/2
DeviceA(config-if-GigabitEthernet0/2)# ip address 152.95.1.2 255.255.255.252
DeviceA(config-if-GigabitEthernet0/2)# ip verify unicast source reachable-via any
DeviceA(config-if-GigabitEthernet0/2)# ip verify urpf drop-rate notify
DeviceA(config-if-GigabitEthernet0/2)# end
```

5. Verification

If source address spoofing exists on the network, run the **show ip urpf** command to display the number of spoofing packets discarded by uRPF.

```
DeviceA# show ip urpf
IP verify URPF drop-rate compute interval is 300s
IP verify URPF drop-rate notify hold-down is 300s
Interface gigabitEthernet0/1
IP verify source reachable-via ANY
IP verify URPF drop-rate notify is enabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 4121
Number of drop-rate notification counts in this interface is 2
Interface gigabitEthernet0/2
IP verify source reachable-via ANY
IP verify URPF drop-rate notify is enabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 352
Number of drop-rate notification counts in this interface is 0
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 ip address 195.52.1.2 255.255.255.252
 ip verify unicast source reachable-via any
 ip verify urpf drop-rate notify
!
interface GigabitEthernet 0/2
 ip address 152.95.1.2 255.255.255.252
 ip verify unicast source reachable-via any
 ip verify urpf drop-rate notify
!
end
```

Contents

1 Configuring DoS Protection 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Configuration Task Summary 3
1.3 Configuring the Function of Denying Land Attacks 3
1.3.1 Overview 3
1.3.2 Procedure 3
1.4 Configuring the Function of Denying Invalid TCP Packets 4
1.4.1 Overview 4
1.4.2 Procedure 4
1.5 Configuring the Function of Denying Invalid L4 Ports 4
1.5.1 Overview 4
1.5.2 Procedure 4
1.6 Configuring the Function of Denying Null Scan Attacks 4
1.6.1 Overview 4
1.6.2 Restrictions and Guidelines 4
1.6.3 Procedure 4
1.7 Configuring the Function of Denying ICMP Flood Packets 4
1.7.1 Overview 4
1.7.2 Restrictions and Guidelines 4
1.7.3 Procedure 5

1.8 Configuring the Function of Denying SYN Flood Packets.....5

1.8.1 Overview 5

1.8.2 Restrictions and Guidelines 5

1.8.3 Procedure.....5

1.9 Configuring Attack Packet Statistics.....5

1.9.1 Overview 5

1.9.2 Restrictions and Guidelines 5

1.9.3 Procedure.....6

1.10 Monitoring 6

1 Configuring DoS Protection

1.1 Introduction

1.1.1 Overview

Denial-of-service (DoS) attacks aim to put computers or networks out of service.

DoS attacks are diversified in types and can be implemented in many ways but have one common purpose, that is, prevent victim hosts or networks from receiving, processing, or responding to external requests in time. In particular, in an L2 network, DoS attack packets can be spread in the entire broadcast domain. If hackers maliciously initiate DoS attacks, some operating systems (OSs) may collapse. Ruijie products support the following anti-DoS attack functions:

- Denying land attacks
- Denying invalid Transmission Control Protocol (TCP) packets
- Denying invalid L4 ports
- Denying null scan attacks
- Denying Internet Control Message Protocol (ICMP) flood packets
- Denying TCP synchronization (SYN) flood packets

1.1.2 Principles

1. Denying Land Attacks

In a land attack, the attacker sets the source and destination IP addresses in an SYN packet to the same address of the target host. Consequently, the attacked host will be trapped in an infinite loop or even collapse when attempting to set up a TCP connection with itself.

When the function of denying land attacks is enabled, the device checks packets based on characteristics of land packets (that is, SYN packets with the same source and destination IP addresses), and discards invalid packets.

2. Denying Invalid TCP Packets

There are several flag fields in the TCP packet header:

- SYN: Connection establishment flag. A TCP SYN packet sets this flag to **1** to request establishment of a connection.
- ACK: Acknowledgment flag. In a TCP connection, this field must be available in every packet (except the first packet, that is, the TCP SYN packet) as the acknowledgment of the previous packet.
- FIN: Finish flag. When a host receives the TCP packet with the FIN flag, the host disconnects the TCP connection.
- RST: Reset flag. When the IP protocol stack receives a TCP packet that contains a non-existent destination port, it responds with a packet carrying the RST flag.
- PSH: This flag notifies the protocol stack to submit TCP data to the upper-layer program for processing as soon as possible.

In invalid TCP packets, flag fields are set improperly to consume processing resources of hosts or even collapse the system. The following lists several common methods for setting flag fields in invalid TCP packets:

- TCP packets with both the SYN and FIN flags

  Normally, a TCP packet cannot contain both the SYN and FIN flags. In addition, RFC does not stipulate how the IP protocol stack should process such invalid packets containing both the SYN and FIN flags. The protocol stack of each OS may process such packets in different ways. Attackers can use this feature to send packets containing both the SYN and FIN flags to identify the OS type and initiate attacks on this OS.

- TCP packets without any flag

  Normally, a TCP packet contains at least one of the five flags, including SYN, FIN, ACK, RST, and PSH. The first TCP packet (TCP SYN packet) must contain the SYN flag, and the subsequent packets contain the ACK flag. Based on such assumptions, some protocol stacks do not specify the method for processing TCP packets without any flag and may collapse if such TCP packets are received. Attackers use this feature to initiate attacks on target hosts.

- TCP packets with the FIN flag but without the ACK flag

  Normally, except the first packet (TCP SYN packet), all other packets, including the packets with the FIN flag, contain the ACK flag. Some attackers may send TCP packets with the FIN flag but without the ACK flag to the target hosts, causing breakdown of the target hosts.

- TCP packets with the SYN flag and the source port ID set to a value between 0 and 1023

  Port IDs 0 to 1023 are known port IDs allocated by the Internet Assigned Numbers Authority (IANA). In most systems, these port IDs can be used only by the system (or root) processes or programs run by privileged users. These ports (0–1023) cannot be used as the source ports in the first TCP packets (with the SYN flag) sent by clients.

  When the function of denying invalid TCP packets is enabled, the device checks packets based on characteristics of invalid TCP packets and discards invalid TCP packets.

3. Denying Invalid L4 Ports

Attackers send packets in which the IP address and L4 port ID are the same as those of the target host to the target host. As a result, the target host sends TCP connection setup requests to itself. Under such attacks, resources of the target host will soon be exhausted and the system will collapse.

When the function of denying invalid L4 ports is enabled, the device checks the L4 source port ID and destination port ID in the packets. If they are the same, the device discards the packets.

4. Denying Null Scan Attacks

Attackers send TCP packets without any flag to the target host IP address. Some OSs proactively respond with RST packets. In this case, attackers can obtain enabled ports. By sending TCP packets without any flag in the data packet header, attackers can generate invalid data packets based on RFC 793 to initiate null scan attacks. The expected behavior in RFC 793 is that TCP packets with incorrect state are sent to enabled ports of the destination host, which will be discarded by the destination host, and TCP packets with the status flag are sent to disabled ports of the destination host, and the destination host will response with RST packets. Attackers may send data packets of some types that violate rules (non-synchronized TCP connection or TCB disallowed) to scan disabled ports and use RST data packets to detect disabled ports.

The new RFC standard can filter out all TCP packets without a flag. Denying null scan attacks is to discard TCP packets without any TCP flag. This effectively prevents attackers from obtaining the disabling status of ports through null scan and initiating subsequent attacks.

5. Denying ICMP Flood Packets

ICMP flood is a distributed denial-of-service (DDoS) attack, which sends many ping packets to the target host in a short period of time to consume resources of the host. After resources of the host are used up, the host will collapse or cannot provide services.

6. Denying SYN Flood Packets

SYN flood is the commonest DDoS attack and also a typical DoS attack in networks. By exploiting TCP implementation defects, it sends many attack packets with forged source addresses to network service ports, which may cause the half-open connection queue of the target server being occupied and prevent other legitimate users from accessing the server.

1.2 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Function of Denying Land Attacks
- Configuring the Function of Denying Invalid TCP Packets
- Configuring the Function of Denying Invalid L4 Ports
-
- Configuring the Function of Denying ICMP Flood Packets
- Configuring the Function of Denying SYN Flood Packets
- Configuring Attack Packet Statistics

1.3 Configuring the Function of Denying Land Attacks

1.3.1 Overview

If the function of denying land attacks is enabled, the device checks packets based on characteristics of land packets (that is, SYN packets with the same source and destination IP addresses), and discards invalid packets.

1.3.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of denying land attacks.

ip deny land

The function of denying land attacks is disabled by default.

1.4 Configuring the Function of Denying Invalid TCP Packets

1.4.1 Overview

When the function of denying invalid TCP packets is enabled, the device checks packets based on characteristics of invalid TCP packets and discards invalid TCP packets.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of denying invalid TCP packets.

ip deny invalid-tcp

The function of denying invalid TCP packets is disabled by default.

1.5 Configuring the Function of Denying Invalid L4 Ports

1.5.1 Overview

When the function of denying invalid L4 ports is enabled, the device checks the L4 source port ID and destination port ID in the packets. If they are the same, the device discards the packets.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of denying invalid L4 ports.

ip deny invalid-l4port

The function of denying invalid L4 ports is disabled by default.

1.6 Configuring the Function of Denying ICMP Flood Packets

1.6.1 Overview

After the function of denying ICMP flood packets is enabled, the device will limit the rate of ICMP packets entering the network and prevent resources of the internal server being excessively consumed by ICMP attack packets.

1.6.2 Restrictions and Guidelines

- Typically, this function is configured on devices connected to the server.
- After this function is enabled, only the rate of bypassing ICMP packets is limited, and ICMP packets sent from the local device to the CPU are not affected.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of denying ICMP flood packets.

ip defense icmp-flood *rate-limit*

The function of denying ICMP flood packets is disabled by default.

1.7 Configuring the Function of Denying SYN Flood Packets

1.7.1 Overview

After the function of denying SYN flood packets is enabled, the device will limit the rate of SYN packets entering the network and prevent resources of the internal server being excessively consumed by SYN attack packets.

1.7.2 Restrictions and Guidelines

- Typically, this function is configured on devices connected to the server.
- After this function is enabled, only the rate of bypassing TCP SYN packets is limited, and TCP SYN packets sent from the local device to the CPU are not affected.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of denying TCP SYN flood packets.

ip defense syn-flood *rate-limit*

The function of denying TCP SYN flood packets is disabled by default.

1.8 Configuring Attack Packet Statistics

1.8.1 Overview

After the attack packet statistics function is enabled, statistics are collected for null scan packets entering the network and bypassing ICMP/SYN flood packets, and interfaces are provided to display permitted and discarded packets on the forwarding plane.

1.8.2 Restrictions and Guidelines

- Typically, this function is configured on devices connected to the server.
- Enabling this function will occupy many underlying hardware resources. Therefore, this function is disabled

by default.

- The device discards null scan attack packets directly. Therefore, only the count of discarded packets will be updated.
- The function can collect statistics of null scan packets and bypass ICMP/SYN flood packets only.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of collecting statistics of null scan packets and ICMP/SYN flood packets.

ip ddos counter enable

The function of collecting statistics of null scan packets and ICMP/SYN flood packets is disabled by default.

1.9 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show ip defense icmp-flood	Displays the status of the function of denying ICMP flood packets.
show ip defense syn-flood	Displays the status of the function of denying TCP SYN flood packets.
show ip deny land	Displays the status of the function of denying land attacks.
show ip deny invalid-tcp	Displays the status of the function of denying invalid TCP packets.
show ip deny invalid-l4port	Displays the status of the function of denying invalid L4 ports.
show ip deny	Displays the status of all anti-DoS attack functions.

Contents

1 Configuring Security Log Auditing 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.2 Restrictions and Guidelines 2
1.3 Configuration Task Summary 2
1.4 Configuring Security Log Auditing 2
1.4.1 Overview 2
1.4.2 Enabling Security Log Auditing 2
1.4.3 Configuring the Local Storage Time for Security Logs 3
1.4.4 Configuring the Handling Time of Aged Security Logs 3
1.4.5 Configuring the Local Storage Capacity for Security Logs 3
1.4.6 Enabling the Function of Sending Security Logs to the Syslog Server 4
1.5 Monitoring 4
1.6 Configuration Examples 5
1.6.1 Configuring Security Log Auditing 5

1 Configuring Security Log Auditing

1.1 Introduction

1.1.1 Overview

Security log auditing is used to record key operations on a device and audit and backtrack these operations afterwards to improve the device security and meet the national security standards.

Instruction

The following sections describe content related to security log auditing only.

1.1.2 Principles

1. Basic Concepts

- Key operation

  After enabling the security log auditing function, the device records logs for key operations, including account management, login events, system events, configuration file changes, and security log events. Key operations include:

  - Adding/deleting accounts
  - Editing authentication information
  - Modifying configurations (such as the DNS address and IP address)
  - User login/logout
  - Restarting/Stopping the device
  - Uploading/downloading files (when supported)
  - Editing user permissions (when supported)
  - Enabling/disabling log auditing and deleting logs

2. Enabling Security Log Auditing

After the security log auditing function is enabled, the device can record logs for key operations and locally store the logs.

When a user performs a key operation, such as account management, login/logout, system restart, configuration file change, or log auditing function enabling/disabling, the corresponding service module will collect information (such as time, username, IP address, operation log content, and operation result), generate a log, and write the log to the local database through the log auditing framework.

At 03:00:00 a.m. each day, the system checks whether any logs for key operations exceed the storage time. If yes, the logs will be deleted.

A maximum of 10,000 logs can be stored by default. After the number of stored logs exceeds the storage limit, new logs will overwrite the earliest ones.

3. Enabling the Function of Sending Security Logs to the Syslog Server

After a device is configured with the functions of syslog, and the security log auditing and sending functions are enabled, the log auditing framework will send generated logs to the syslog server to store.

1.2 Restrictions and Guidelines

- To protect the flash storage chip, newly generated logs will be cached in the memory and written to a file every 1 hour. When a restart command, such as **reload**, is executed, logs will be written to a file. If many logs are generated in this hour and some logs are not written to the file in 1 hour, the logs will be lost.
- When logs are exported to a file, download the file in time. The file will be automatically deleted after 1 hour.

1.3 Configuration Task Summary

Configuration of security log auditing includes the following tasks:

(1) Enabling Security Log Auditing

(2) (Optional) Configuring the Local Storage Time for Security Logs

(3) (Optional) Configuring the Handling Time of Aged Security Logs

(4) (Optional) Configuring the Local Storage Capacity for Security Logs

(5)

1.4 Configuring Security Log Auditing

1.4.1 Overview

The security log auditing function can record logs for key operations on a device and locally store the logs. Log query and export are supported.

1.4.2 Enabling Security Log Auditing

1. Overview

After the security log auditing function is enabled, the device will record logs for key operations, including account management, login events, system events, configuration file changes and security log events, and store the logs to the local database.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable security log auditing.

security-log audit-enable

Security log auditing is enabled by default.

1.4.3 Configuring the Local Storage Time for Security Logs

1. Overview

After the local storage time is configured for security logs, the logs that have exceeded the storage time will be deleted.

2. Restrictions and Guidelines

Security logs that have exceeded the storage time will be deleted.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the local storage time for security logs.

security-log data-store-days *data-store-time*

The default local storage time for security logs is **65535** days.

1.4.4 Configuring the Handling Time of Aged Security Logs

1. Overview

After the handling time of aged security logs is configured, the system checks whether any logs have exceeded the storage time at the configured handling time (deviation: 5 minutes) and deletes expired logs.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the handling time of aged security logs.

security-log auto-vacuum-time *hh*:*mm*:*ss*

The default handling time of aged security logs is **03:00:00** every day.

1.4.5 Configuring the Local Storage Capacity for Security Logs

1. Overview

After the local storage capacity for security logs is configured, new logs will overwrite earliest ones when the capacity of locally stored logs exceeds the storage limit.

2. Restrictions and Guidelines

If flash space is limited, you can run this command to decrease the storage capacity for security logs.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the local storage capacity for security logs.

security-log data-store-items *log-number*

The default local storage capacity for security logs is **10000**.

1.5 Monitoring

Run the **delete** commands to clear information.

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** commands to output debugging information.

Notice

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
debug security-log errors	Debugs log auditing.
debug security-log recv-info	Debugs received logs.
debug security-log sql-info	Debugs the log database.
show security-log	Displays all logs.
show security-log config	Displays configurations.
show security-log detail { **all** | { **from** *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss* } } [**hostname** *hostname*] [**log-type** { **ACC_MNT** | **CONFIG** | **LOGIN** | **OTHER** | **SEC_LOG** | **SYS** }] [**peerinfo** *peerinfo*] [**user** *username*] { [**order-by** { **log-type** | **time** } { **asc** | **desc** } [**start-item** *start-item* **end-item** *end-item*]] }	Displays the detailed log information, which can be filtered by time, log type, username, host name, and terminal information.
show security-log detail export { **all** | { **from** *YY//MM/DD hh*:*mm*:*ss* **to** *YY//MM/DD hh*:*mm*:*ss* } } [**hostname** *hostname*] [**log-type** { **ACC_MNT** | **CONFIG** | **LOGIN** | **OTHER** | **SEC_LOG** | **SYS** }] [**peerinfo** *peerinfo*] [**user** *username*] { [**order-by** { **log-type** | **time** } { **asc** | **desc** } [**start-item** *start-item* **end-item** *end-item*]] }	Exports the detailed log information, which can be filtered by time, log type, username, host name, and terminal information.

Command	Purpose
show security-log detail stat { **all** | { **from** *YY//MM/DD hh:mm:ss* **to** *YY//MM/DD hh:mm:ss* } } [**hostname** *hostname*] [**log-type** { **ACC_MNT** | **CONFIG** | **LOGIN** | **OTHER** | **SEC_LOG** | **SYS** }] [**peerinfo** *peerinfo*] [**user** *username*]	Displays the log statistics, which can be filtered by time, log type, username, host name, and terminal information.
show security-log info	Displays the statistics during log processing.
show security-log statistics	Displays the statistics.
security-log delete all	Deletes all logs.

1.6 Configuration Examples

1.6.1 Configuring Security Log Auditing

1. Requirements

To improve device security and audit and backtrack exceptions (such as key configurations being tampered) afterwards, key operations on a device need to be recorded. After the security log auditing function is enabled, the device records key operations, including account management, login events, system events, configuration file changes, and security log events. After logging in to the device, the administrator can monitor recent user behaviors through the records.

2. Topology

Figure 1-1 Configuring Security Log Auditing

3. Notes

- Enable security log auditing.
- Configure parameters related to security log auditing.

4. Procedure

Enable security log auditing.

```
Device> enable
Device# configure terminal
Device(config)# security-log audit-enable
```

Set the local storage time of security logs to **300** days.

```
Device(config)# security-log data-store-days 300
```

Set the handling time of aged security logs to **05:05:00** every day.

```
Device(config)# security-log auto-vacuum-time 05:05:00
```

Set the local storage capacity for security logs to **1000**.

```
Device(config)# security-log data-store-items 1000
```

5. Verification

Log in to the device, perform key operations, and run **show security-log detail all** 30s later to check the log auditing records.

```
Device# show security-log detail all
time, username, peerinfo, hostname, log-type: content
2019-10-22 10:00:02, admin, vty0(192.168.111.111), Device, SEC_LOG: SECURITY_LOG
deleted all security log successfully
2019-10-22 10:00:02, admin, vty0(192.168.111.111), Device, SEC_LOG: SECURITY_LOG
disabled security log audit configuration unsuccessfully
2019-10-22 10:00:03, ---, console, Device, SEC_LOG: SECURITY_LOG enabled security
log audit configuration successfully
```

Run the **show security-log config** command to verify that the local storage time of security logs is 300 days, the handling time of aged security logs is 05:05:00 every day, and the local storage capacity for security logs is 1000.

```
Device# show security-log config
Security-log audit: enable
Limit number: 10000
Store days: 300
Auto vacuum time: 05:05:00
```

6. Configuration Files

Device configuration file

```
hostname Device
!
security-log data-store-days 300
security-log data-store-items 1000
security-log auto-vacuum-time 05:05:00
!
end
```

Reliability Configuration

1. REUP Configuration
2. RLDP Configuration
3. DLDP Configuration
4. VRRP Configuration
5. VRRP Plus Configuration
6. BFD Configuration
7. Track Configuration
8. IP Event Dampening Configuration
9. HAM Configuration

Contents

1 Configuring REUP 1
1.1 Introduction 1
1.1.1 Topology 1
1.1.2 Basic Concepts 2
1.1.3 Dual-Link Backup 2
1.1.4 MAC Address Update 4
1.1.5 VLAN Load Balancing 5
1.1.6 Link State Tracking 6
1.2 Configuration Task Summary 7
1.3 Configuring Basic Features of REUP 8
1.3.1 Overview 8
1.3.2 Restrictions and Guidelines 8
1.3.3 Procedure 8
1.4 Configuring the Preemption Function of REUP 8
1.4.1 Overview 8
1.4.2 Restrictions and Guidelines 9
1.4.3 Procedure 9
1.5 Configuring the MAC Address Update Function 9
1.5.1 Overview 9
1.5.2 Restrictions and Guidelines 10
1.5.3 Procedure 10
1.6 Configuring VLAN Load Balancing 11

1.6.1 Overview 11

1.6.2 Restrictions and Guidelines 11

1.6.3 Procedure 11

1.7 Configuring Link State Tracking 12

1.7.1 Overview 12

1.7.2 Restrictions and Guidelines 12

1.7.3 Procedure 12

1.8 Monitoring 12

1.9 Configuration Examples 13

1.9.1 Configuring Basic Features of REUP 13

1.9.2 Configuring the MAC Address Update Function 16

1.9.3 Configuring VLAN Load Balancing 19

1.9.4 Configuring Link State Tracking 22

1 Configuring REUP

Rapid Ethernet Uplink Protection (REUP) provides a rapid uplink protection function. In the dual uplink networking, REUP is used to ensure normal communication between links, block redundant links, avoid link loops, and implement fast backup.

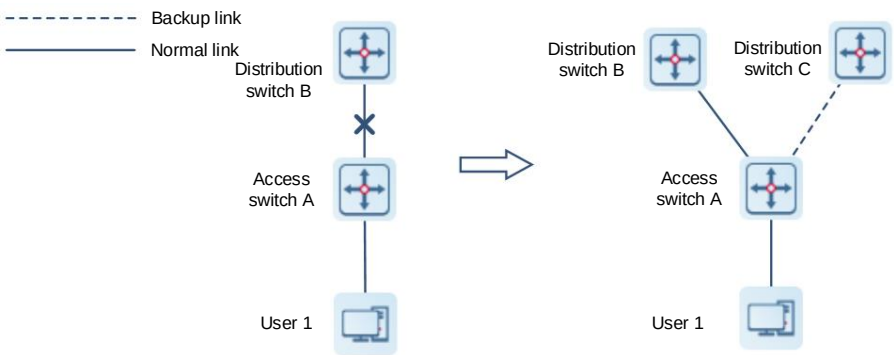
1.1 Introduction

1.1.1 Topology

The left topology in Figure 1-1 shows single uplink networking, where there is only one link between the user and the distribution switch to implement communication. When the link between access switch A and distribution switch B fails, the link between the user and switch B is disconnected, which interrupts all external services of the user.

The topology can be transformed into REUP dual uplink deployment topology, as shown in the right topology in Figure 1-1. In this topology, one link functions as the active link for normal communication, and the other link functions as a backup link and is not used for communication. When the active link fails, traffic is switched to the backup link. This helps reduce the impact of a single link failure on the network and improve reliability.

Figure 1-1 REUP Topology



REUP and the Spanning Tree Protocol (STP) are mutually exclusive on ports. Generally, a device runs STP in the downlink direction and runs REUP in the uplink direction to implement uplink backup and data protection in the case of faults. REUP can still provide basic link redundancy when STP is disabled. It also provides millisecond-level fault recovery faster than STP. Its main features are as follows.

- The uplink ports of REUP are configured in pairs, namely, an uplink port pair includes a forward port and a standby port. The standby port does not forward data packets. When the forward port fails, the standby port immediately becomes the forward port to forward data.
- REUP sends an address update packet to the upstream device so that the upstream device can update the MAC address information immediately. This function ensures that L2 data streams are restored rapidly after a link gets faulty.

1.1.2 Basic Concepts

1. REUP Pair

You can specify a port as the backup port of another port to configure an REUP pair, in which one port is the active port and the other is the backup port. When both ports are normal, one port is configured as the forward port and the other as the standby port.

2. MAC Address Update Message

According to the MAC address learning principle, before L2 link switching a user's MAC address entry exists on the forwarding link, and no packet is forwarded by the blocked link, so there is no user's MAC address entry on the blocked link. After switching, packets cannot be forwarded because they are still forwarded according to the existing MAC address entry of the user. MAC address update messages refer to FLUSH packets sent to an uplink device through private multicast packets. When an uplink device, on which the function of receiving MAC address update messages is enabled, receives a MAC address update message, the device updates the MAC entry on the relevant interface.

3. MAC Address Update Group

Multiple ports can be added to a group. If one port in the group receives a MAC address update message, the MAC address entries on other ports in the group are updated at the same time. In this case, the group is called a MAC address update group.

4. MAC Address Update Packet

MAC address update packets are sent to uplink devices of other manufacturers to ask them to update their MAC address entries, so as to implement compatibility with them.

5. Link State Tracking Group

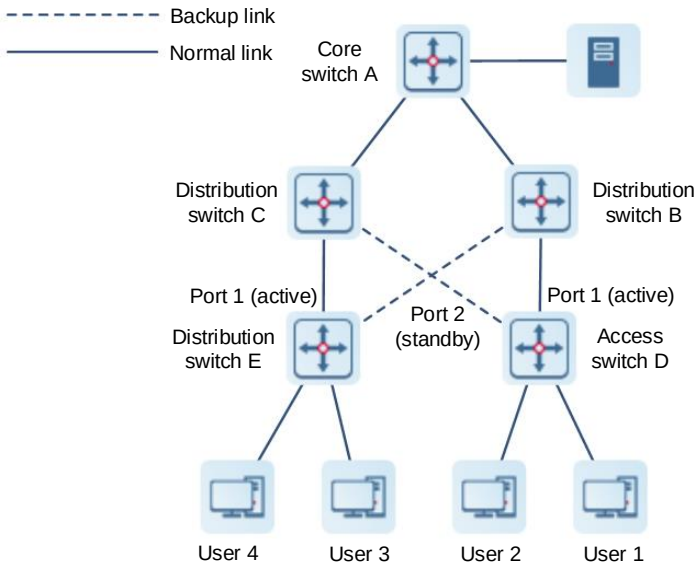
The uplink and downlink ports of a device can be added to a group at the same time, which is called a link state tracking group. If all uplink ports in the group are down, all downlink ports in this group are forced down.

1.1.3 Dual-Link Backup

When an active link is faulty, the link in the backup state will rapidly switch to the forward state and start to forward data, to minimize the service interruption caused by the link failure. REUP adopts the real-time backup and batch backup mechanisms to ensure that the configuration and operating status of the standby device are completely consistent with those of the active device. When the master/slave switching occurs in a virtual switch unit (VSU) scenario, the data flow is not cut off, the operating status of REUP is consistent with that before the switching, and link switching is not performed again.

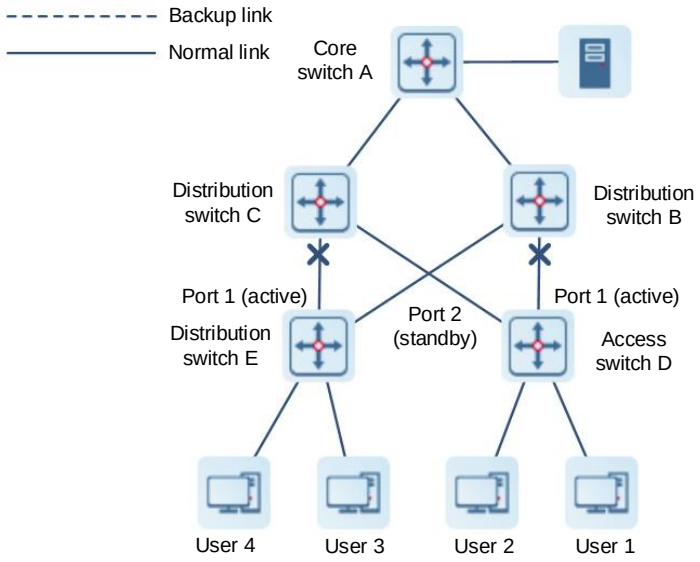
- You can specify a port as the backup port of another port to configure an REUP pair. When the two ports are normal, one link is in the forwarding state (forwarding data packets) and the other link is in the backup state (not forwarding data packets).
- When the active link is faulty, the link in the backup state rapidly switches to the forwarding state and starts to forward data.
- When the faulty link recovers, it enters the backup state and does not forward data packets.
- The preemption mode can be configured to specify whether the link recovering from a fault preempts to become the link in the forwarding state.

Figure 1-2 Topology with Two Normal Links



As shown in Figure 1-2, ports 1 and 2 of switch D (switch E) are connected to uplink switches B and C (switches C and B) respectively, and REUP is configured on ports 1 and 2. When the links are normal, port 1 is in the forwarding state and forwards data packets and port 2 is in the backup state and does not forward data packets.

Figure 1-3 Topology with Faulty Port 1 of Switch D (Switch E)



As shown in Figure 1-3, once port 1 fails, port 2 immediately starts to forward data packets and restores uplink transmission of the switch. In the non-preemption mode, when the link of port 1 recovers, port 1 is in the backup state and does not forward data packets, and port 2 continues forwarding data packets. You must enable the REUP dual-link backup function on a port so that the port undertakes the REUP link switching when the port is faulty.

Note

- REUP, Ethernet Ring Protection Switching (ERPS), and Rapid Ethernet Ring Protection (RERP) do not share ports.
- On devices enabled with REUP, the storm control function must be disabled on all L2 ports.

1.1.4 MAC Address Update

During link switching, the MAC address entries on a port are updated to speed up packet convergence. As shown in Figure 1-2, the MAC address update process is analyzed as follows:

- Ports 1 and 2 of switch D (switch E) have the REUP dual-link backup enabled. Port 1 works as the active port. During normal communication, switch A learns the MAC addresses of users 1 and 2 (users 3 and 4) from the port connecting to switch B (switch C).
- When port 1 of switch D (switch E) fails, port 2 quickly changes to the forwarding state and starts to forward data packets. In this case, switch A has not learned the MAC addresses of users 1 and 2 (users 3 and 4) from the port connecting to switch B (switch C). The data packets sent by the server to users 1 and 2 (users 3 and 4) are forwarded to switch C (B) by switch A, causing loss of the packets from the server to users 1 and 2 (users 3 and MAC 4).

The following measures can be taken to avoid the above problem:

- Enable the MAC address update function on switch D (switch E). When port 2 starts to forward packets, switch D (switch E) sends a MAC address update message to port 2.
- After receiving the MAC address update message from port 2, switch A updates the MAC address entries on the port of switch A. In this way, switch A forwards the packets sent by the server to the users, to the port connecting to switch C (switch B) to speed up packet transmission convergence.
- In addition, a MAC address update group can be configured, that is, multiple ports can be classified into the same group. When a port in this group receives a MAC address update message, the MAC address entries on other ports in the group are updated, to reduce the side effect of flooding caused by MAC address update.
- To be compatible with upstream devices not supporting MAC address update messages, switch D (switch E) sends MAC address update packets for users 1 and user 2 (users 3 and 4) upstream when port 2 switches to the forwarding state. In this way, switch A updates the MAC addresses of users 1 and 2 (users 3 and 4) to the corresponding port and the downstream data transmission of switch A is restored.

Based on the above process analysis, the relevant configuration to be involved includes the following items:

Table 1-1 Description of MAC Address Update Configuration Items

Configuration Item	Description
Sending MAC address updates	If the function of sending MAC address update messages is not enabled, no MAC address update message is sent when REUP dual-link backup switching is performed.

Configuration Item	Description
Receiving MAC address updates	If the function of receiving MAC address update messages is not enabled, a device cannot receive MAC address update messages from downlink devices during REUP dual-link backup switching and will not update the MAC addresses.
Specifying a VLAN for sending MAC address updates	If the VLAN in which an interface sends MAC address update messages is configured, the messages are sent in the configured VLAN; otherwise, the messages are sent in the default VLAN to which the interface belongs.
Specifying a VLAN for receiving MAC address updates	If no VLAN in which an interface receives MAC address update messages is configured, MAC address update messages are received in all the configured VLANs; otherwise, MAC address update messages are received in the specified VLAN.
MAC address update group	If no MAC address update group is configured, MAC address update is not performed when MAC address update packets are received.
Maximum number of MAC address update messages sent per second	A greater number of messages configured indicates more CPU time used for sending messages and fewer downstream packets to be lost.

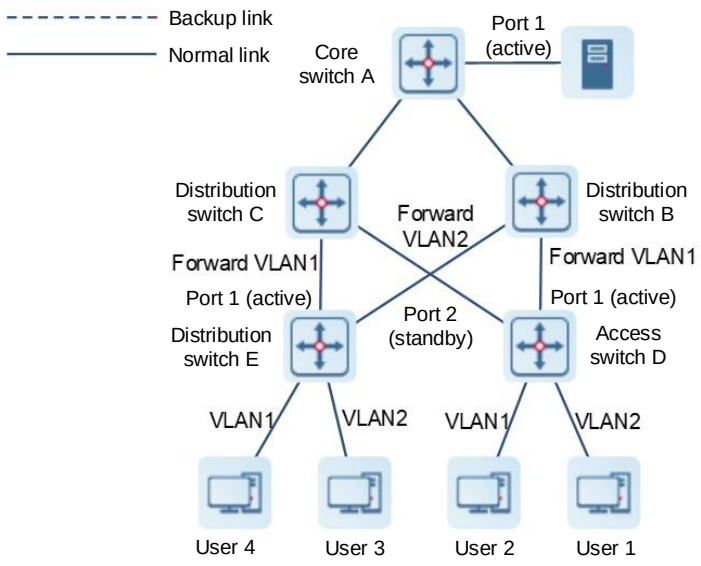
1.1.5 VLAN Load Balancing

The VLAN load balancing function allows the two ports of a REUP pair to forward data packets of mutually exclusive VLANs so as to make full use of the link bandwidth.

As shown in Figure 1-4, the MAC address update process is analyzed as follows:

- Configure REUP dual-link backup and enable the VLAN load balancing of REUP on ports 1 and 2 of switch D, and map VLAN 1 to instance 1 and VLAN 2 to instance 2. Data of VLAN 1 (instance 1) is transmitted through port 1 and data of VLAN 2 (instance 2) is transmitted through port 2. Perform the same configuration on switch E.
- When a port is faulty, the other port takes over the transmission of all VLAN data.
- When the faulty port recovers and works properly within the preemption delay, the transmission of VLAN data in the charge of the faulty port is switched back to the recovered port.

Figure 1-4 Load Balancing Topology with Two Normal Links



Therefore, the VLAN load balancing function needs to be enabled on the ports to make full use of the link bandwidth for packet forwarding when both links are normal.

Caution

- The instance mapping of REUP VLAN load balancing is controlled by the Multiple Spanning Tree Protocol (MSTP) module in a unified manner. For details about how to configure the instances, see "Configuring MSTP" in *Ethernet Switching Configuration Guide*.
- The VLAN load balancing function can be configured only on trunk, uplink, or hybrid ports.

1.1.6 Link State Tracking

Link state tracking means that, when an upstream link is faulty, the downstream link switches services to the backup upstream link so that the backup port can continue to forward packets. Link state tracking provides the function of notifying a downlink device to perform link switching when all the upstream links are faulty. You can configure the upstream and downstream ports of a link state tracking group and bind the link states of multiple downstream ports to multiple uplink ports to implement link state synchronization. When all uplinks in a tracking group are faulty, the downlink ports are shut down forcibly to ensure that the downlink transmission is switched from the active link to the backup link.

As shown in Figure 1-5, when the uplink of switch B is faulty, link state tracking rapidly shuts down the downstream port of switch B so that the upstream transmission of switch D is switched to switch C.

Figure 1-5 Topology with the Active Uplink Faulty

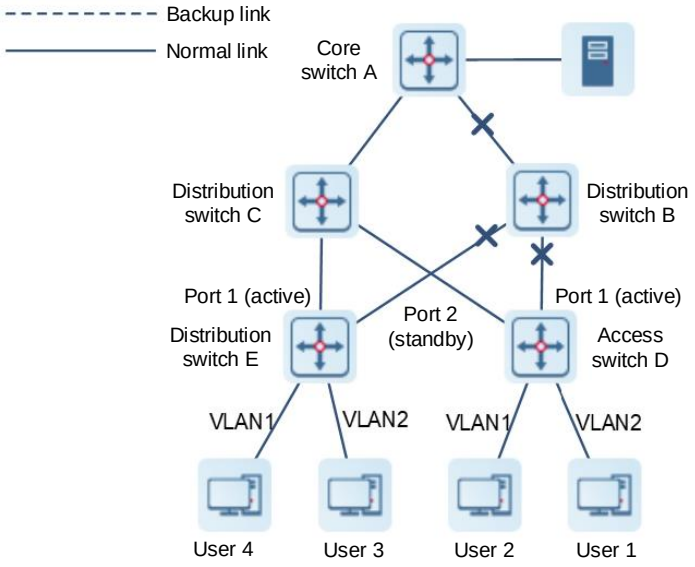


Table 1-2 Description of Link State Tracking Configuration Items

Configuration Item	Description
Link state tracking function	If the link state tracking function is not enabled, the state of a corresponding uplink port cannot be detected and packet forwarding switching cannot be implemented in time.
Downlink up delay function for a link state tracking group	By enabling the downlink up delay function, you can avoid frequent downlink switching caused by uplink flapping in a link state tracking group. That is, when the uplink becomes up, the downlink becomes up after a delay.
Adding a port to a link state tracking group	If a port is not added to a link state tracking group, the state of a corresponding uplink port cannot be detected and packet forwarding switching cannot be implemented in time.

1.2 Configuration Task Summary

REUP configuration includes the following tasks:

(1) Configuring Basic Features of REUP

(2) (Optional) Configuring the Preemption Function of REUP

(3) Configuring the MAC Address Update Function

(4) (Optional) Configuring VLAN Load Balancing

(5) Configuring Link State Tracking

1.3 Configuring Basic Features of REUP

1.3.1 Overview

When a link is faulty, another normal link switches to the forward state immediately to forward packets.

1.3.2 Restrictions and Guidelines

- One port belongs to only one REUP pair. Each active link has only one backup link. A backup link can be used as the backup link of only one active link. The active and backup links must use different ports.
- REUP supports L2 physical ports and L2 aggregate ports (APs), but does not support AP member ports.
- The active and backup ports may be of different types and have different rates. For example, an AP can be used as the active port and a physical port can be configured as the backup port.
- Ports configured with REUP are not involved in STP calculation.
- Each device can be configured with a maximum of 16 REUP pairs.
- Ports successfully configured with REUP cannot be configured as L3 ports or added to an AP.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a REUP dual-link backup port.

switchport backup interface *interface-type interface-number*

No REUP dual-link backup port is configured by default.

1.4 Configuring the Preemption Function of REUP

1.4.1 Overview

- If the active link needs to always forward packets or the link for forwarding packets needs to be determined based on the link bandwidth, the preemption mode and delay time must be configured.
- You can determine the link to be used by configuring the preemption mode. If the preemption mode is set to bandwidth mode, a link with a greater bandwidth is used. The value of the bandwidth attribute of an AP is the actual bandwidth of the AP, equal to the number of link up member ports of the AP multiplied by the speed attribute value of an AP member port. You can also set the preemption mode to forced mode to select a stable and reliable link forcibly.
- To avoid frequent active/backup link switching caused by faults, REUP provides a preemption delay function. After the two links recover, link switching is delayed (**35** seconds by default) for the faulty link to become stable. A smaller delay means more frequent preemption switching after the faulty link recovers. When STP is enabled on an uplink, the preemption delay time of REUP should be greater than 35 seconds.

- The preemption mode can be set to three modes: forced, bandwidth, and off. In the bandwidth mode, a port with a greater bandwidth is selected to transmit data; in the forced mode, the active port is selected to transmit data; in the off mode, no preemption is performed.

1.4.2 Restrictions and Guidelines

REUP dual-link backup must be configured.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the preemption mode of REUP.

switchport backup interface *interface-type interface-number* **preemption mode** { **bandwidth** | **forced** | **off** }

The default link preemption mode of REUP is off mode.

(5) Configure the preemption delay time of REUP.

switchport backup interface *interface-type interface-number* **preemption delay** *interval*

The default preemption delay time of REUP is **35** seconds.

1.5 Configuring the MAC Address Update Function

1.5.1 Overview

- The MAC address update function can rapidly delete and update MAC address information on interfaces during link switching to make packet convergence faster.
- To reduce data loss in downstream data stream during link switching, you need to enable the function of sending MAC address update messages on a switch that performs switching.
- During link switching, REUP sends a certain number of MAC address update packets to an uplink device per second to recover the downstream data transmission of the uplink device.
- When dual-link backup switching occurs, downstream data streams may be lost because the MAC address table of the uplink switch is not updated in time. In order to reduce loss of L2 data streams, you need to update the MAC address table of the uplink switch. In this case, you need to enable the function of receiving MAC address update messages on the uplink switch.
- To reduce massive flooding caused by MAC address update, which may affect normal data transmission of the switch, you can configure a MAC address update group. Only after all ports in a switching path are added to the same MAC address update group, can transmission of downstream data be rapidly recovered.
- For a VLAN in which the function of processing MAC address update messages is disabled, MAC address update packets can be used to recover the downlink transmission of uplink devices; however, the convergence performance will be decreased in the case of link faults.

- After the function of sending MAC address update messages is enabled, MAC address update messages are sent to uplink devices during link switching.

1.5.2 Restrictions and Guidelines

- REUP dual-link backup must be configured.
- A maximum of eight address update groups can be configured on each device. Each address update group can contain a maximum of eight member ports and a port can belong to multiple address update groups.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of sending MAC address update private multicast messages.

mac-address-table move update transit

No MAC address update private multicast message is sent by default.

(4) (Optional) Configure the maximum rate for sending MAC address update broadcast packets.

mac-address-table move update max-update-rate *packet-per-second*

The default maximum rate for sending MAC address update broadcast packets is **150** packets/second.

(5) On an uplink device, enable the function of receiving MAC address update private multicast messages.

mac-address-table move update receive

No MAC address update private multicast message is received by default.

(6) (Optional) On an uplink device, configure the VLAN ID range, in which MAC address update private multicast messages are received.

mac-address-table move update receive vlan *vlan-range*

The MAC address update private multicast messages in all the VLAN ID ranges are received by default.

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Configure the MAC address update group ID for the interface.

mac-address-table update group [*group-id*]

No MAC address update group is configured by default.

(9) (Optional) Configure the ID of a VLAN, in which a port sends MAC address update private multicast messages.

mac-address-table move update transit vlan *vlan-id*

By default, the ID of the VLAN, in which a port sends MAC address update private multicast messages is the local default VLAN of the port.

1.6 Configuring VLAN Load Balancing

1.6.1 Overview

- This function is used to maximize the utilization of link bandwidth.
- You can modify the mapping between instances and VLANs by using the instance mapping function of MSTP.
- The VLAN load balancing function allows the two ports of a REUP pair to forward data packets of mutually exclusive VLANs so as to make full use of the link bandwidth. That is, it allows some VLAN data packets to be forwarded through the backup link, but the active link does not forward these VLAN data packets. In this way, the active link and backup link forward different VLAN data packets and achieve load sharing.
- The VLAN load balancing of REUP relies on the mappings between VLANs and MSTP instances, and the instance mappings are controlled by the MSTP module in a unified manner. For details about how to configure the instances, see the description in "Configuring MSTP."

1.6.2 Restrictions and Guidelines

- REUP dual-link backup must be configured.
- VLAN load balancing cannot be configured on an access port but can share a port with STP.
- For ports successfully configured with VLAN load balancing, you cannot modify the port attributes but can modify the VLAN attributes of the ports.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a group of VLANs.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

(4) Return to the global configuration mode.

exit

(5) Enter the MST configuration mode.

spanning-tree mst configuration

(6) Configure the mappings between instances and VLANs, and add the VLAN group to one MST instance.

instance *instance-id* **vlan** *vlan-range*

Only instance **0** exists and all VLANs belong to instance **0** by default.

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Configure the VLAN load balancing function.

switchport backup interface *interface-type interface-number* **prefer instance** *instance-range*

The VLAN load balancing function is not configured by default.

1.7 Configuring Link State Tracking

1.7.1 Overview

- After detecting that the uplink is disconnected, REUP forcibly disconnects the downlink so that link switching can be performed.
- You must create a link state tracking group first and then add a port to the tracking group.
- You must enable the delay function so that the downlink can be up after the delay.

1.7.2 Restrictions and Guidelines

- REUP dual-link backup must be configured.
- For the link state tracking function, each port belongs to only one link state tracking group and each device can be configured with up to two link state tracking groups. Each link state tracking group can have 8 upstream ports and 256 downstream ports.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable a link state tracking group.

link state track [*track-number*]

All the link state tracking groups are disabled by default.

(4) Configure the downlink recovery delay time for the link state tracking group.

link state track *track-number* **up-delay** *interval*

The downlink of a link state tracking group recovers without delay by default.

(5) Enter the interface configuration mode.

interface *interface-type interface-number*

(6) Add a port to the link state tracking group, and specify it as the uplink port of the group.

link state group *track-number* **upstream**

No port is added to a link state tracking group by default.

(7) Add a port to the link state tracking group and specify it as the downlink port of the group.

link state group *track-number* **downstream**

No port is added to a link state tracking group by default.

1.8 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-3 REUP Monitoring

Command	Purpose
show interfaces [*interface-type interface-number*] **switchport backup** [**detail**]	Displays the REUP dual-link backup information.
show mac-address-table update group [**detail**]	Displays the configurations of a MAC address update group.
show mac-address-table move update	Displays the statistics on MAC address update messages sent by an REUP pair.
show link state group	Displays the information about a link state tracking group.
debug reup all	Debugs all functions of REUP.
debug reup process	Debugs the normal running process of REUP.
debug reup packet	Debugs MAC address update messages of REUP.
debug reup macupdt	Debugs MAC address update packets of REUP.
debug reup ha	Debugs hot backup.
debug reup error	Debugs errors occurring in REUP running.
debug reup event	Debugs received events.
debug reup status	Debugs statistics displayed when a show command is executed.

1.9 Configuration Examples

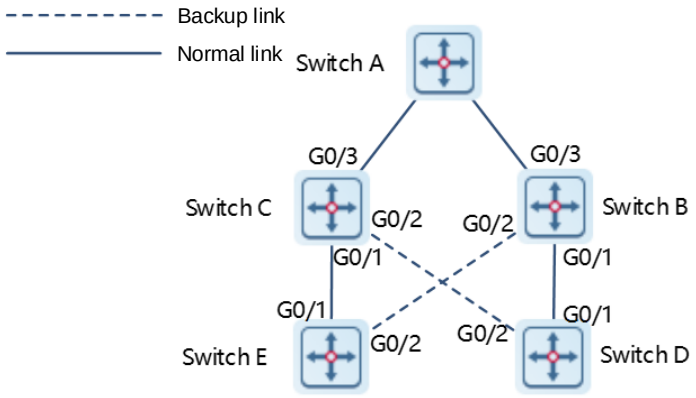
1.9.1 Configuring Basic Features of REUP

1. Requirements

An L3 device networking topology need to be built to simulate the scenario, in which there are two interconnection links between the access devices and the core devices.

2. Topology

Figure 1-6 Topology for Configuring Basic Features of REUP



3. Notes

- Configure REUP dual-link backup (GigabitEthernet 0/1 is the active port and GigabitEthernet 0/2 is the backup port) on access switch D (switch E).

4. Procedure

Perform the following configuration on switch D.

```
SwitchD> enable
SwitchD# configure terminal
SwitchD(config)# interface gigabitethernet 0/1
SwitchD(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchD(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

Perform the following configuration on switch E.

```
SwitchE> enable
SwitchE# configure terminal
SwitchE(config)# interface gigabitethernet 0/1
SwitchE(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchE(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

5. Verification

Run the **show interfaces switchport backup detail** command to verify that the configuration is correct.

Check the configuration of switch D.

```
SwitchD#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------------
```

```
Gi0/1                Gi0/2                Active Up/Backup Standby

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : off
Preemption Delay : 35 seconds
Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)
```

Check the configuration of switch E.

```
SwitchE#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------------
Gi0/1                Gi0/2                Active Up/Backup Standby

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : off
Preemption Delay : 35 seconds
Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)
```

6. Configuration Files

- Switch D configuration file

```
hostname SwitchD
!
interface GigabitEthernet 0/1
 switchport mode trunk
 switchport backup interface GigabitEthernet 0/2
!

end
```

- Switch E configuration file

```
hostname SwitchE
!
interface GigabitEthernet 0/1
 switchport mode trunk
 switchport backup interface GigabitEthernet 0/2
!

end
```

7. Common Errors

- When a port is added to an REUP pair, the port has been configured to belong to another REUP pair.
- A configured port is not an L2 physical port or L2 AP.

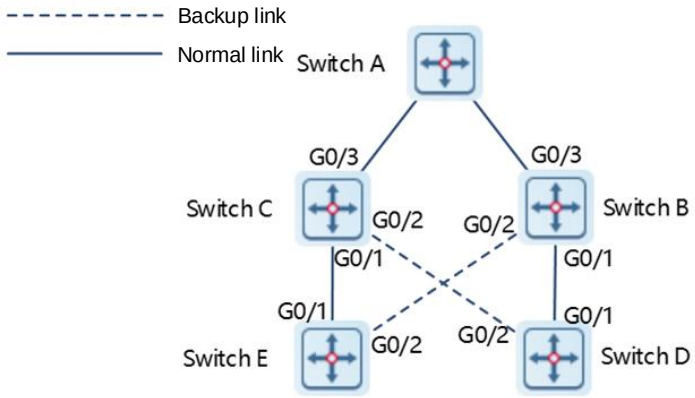
1.9.2 Configuring the MAC Address Update Function

1. Requirements

An L3 device networking topology need to be built to simulate the scenario, in which there are two interconnection links between the access devices and the core devices.

2. Topology

Figure 1-7 Topology for Configuring the MAC Address Update Function



3. Notes

- Enable the function of sending MAC address update messages on access switch D (switch E).
- Enable the function of receiving MAC address update packets on switch B (switch C).
- Add all ports in the REUP switching path to the same MAC address update group.
- Gi0/1 and Gi0/3 of switch B are the ports in the uplink switching path of switch D, and Gi0/3 and Gi0/2 are the ports in the uplink switching path of switch E. You can add ports Gi0/1, Gi0/2, and Gi0/3 to the same address update group. Similarly, you can perform the configuration on switch C.
- Enable the function of receiving MAC address update packets on switch A.
- Add all ports in the REUP switching path of switch A to the same MAC address update group.

4. Procedure

Perform the following configuration on switch D.

```
SwitchD> enable
SwitchD# configure terminal
SwitchD(config)# mac-address-table move update transit
```

Perform the following configuration on switch E.

```
SwitchE> enable
SwitchE# configure terminal
SwitchE((config)# mac-address-table move update transit
```

Perform the following configuration on switch B.

```
SwitchB> enable
SwitchB# configure terminal
```

```
SwitchB(config)# mac-address-table move update receive
SwitchB(config)# interface range gigabitethernet 0/1-3
SwitchB(config-if-range)# switchport mode trunk
SwitchB(config-if-range)# mac-address-table update group 1
```

Perform the following configuration on switch C.

```
SwitchC> enable
SwitchC# configure terminal
SwitchC(config)# mac-address-table move update receive
SwitchC(config)# interface range gigabitethernet 0/1-3
SwitchC(config-if-range)# switchport mode trunk
SwitchC(config-if-range)# mac-address-table update group 1
```

Perform the following configuration on switch A.

```
SwitchA> enable
SwitchA# configure terminal
SwitchA(config)# mac-address-table move update receive
SwitchA(config)# interface range gigabitethernet 0/1-2
SwitchA(config-if-range)# switchport mode trunk
SwitchA(config-if-range)# mac-address-table update group 1
```

5. Verification

Run the **show running** command to check the information about the address update groups on switches D, E, C, B, and A.

```
SwitchD# show run | incl mac-ad
mac-address-table move update transit
```

```
SwitchE# show run | incl mac-ad
mac-address-table move update transit
```

```
SwitchB# show mac-address-table update group detail
show mac-address-table update group detailMac-address-table Update Group:1
Received mac-address-table update message count:0
Group member        Receive Count   Last Receive Switch-ID      Receive Time
--------------------------------------------------------------------------------
Gi0/1             0             0000.0000.0000
Gi0/2             0             0000.0000.0000
Gi0/3             0             0000.0000.0000
```

```
SwitchC# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0
Group member        Receive Count   Last Receive Switch-ID      Receive Time
--------------------------------------------------------------------------------
Gi0/1             0             0000.0000.0000
```

```
Gi0/2             0             0000.0000.0000
Gi0/3             0             0000.0000.0000
```

```
SwitchA# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0
Group member        Receive Count   Last Receive Switch-ID      Receive Time
--------------------------------------------------------------------------------
Gi0/1             0             0000.0000.0000
Gi0/2             0             0000.0000.0000
```

6. Configuration Files

- Switch A configuration file

```
hostname SwitchA
!
interface GigabitEthernet 0/1
 switchport mode trunk
 mac-address-table update group 1
!
interface GigabitEthernet 0/2
 switchport mode trunk
 mac-address-table update group 1
!
mac-address-table move update receive

end
```

- Switch B configuration file

```
hostname SwitchB
!
interface GigabitEthernet 0/1
 switchport mode trunk
 mac-address-table update group 1
!
interface GigabitEthernet 0/2
 switchport mode trunk
 mac-address-table update group 1
!
interface GigabitEthernet 0/3
 switchport mode trunk
 mac-address-table update group 1
!
mac-address-table move update receive

end
```

- Switch C configuration file

```
hostname SwitchC
!
interface GigabitEthernet 0/1
 switchport mode trunk
 mac-address-table update group 1
!
interface GigabitEthernet 0/2
 switchport mode trunk
 mac-address-table update group 1
!
interface GigabitEthernet 0/3
 switchport mode trunk
 mac-address-table update group 1
!
mac-address-table move update receive

end
```

- Switch D configuration file

```
hostname SwitchD
!
mac-address-table move update transit

end
```

- Switch E configuration file

```
hostname SwitchE
!
mac-address-table move update transit

end
```

7. Common Errors

- A configured port is not an L2 physical port or L2 AP.

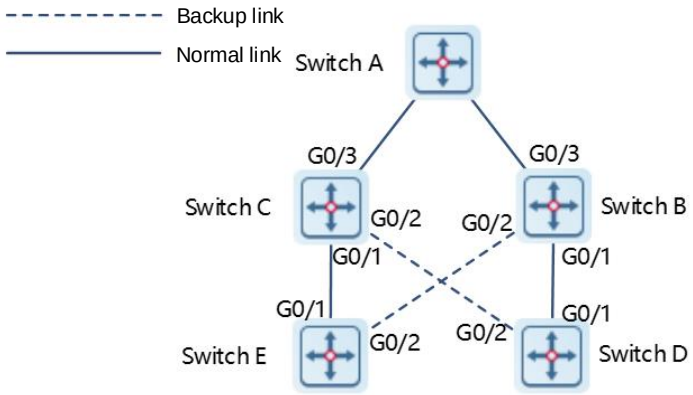
1.9.3 Configuring VLAN Load Balancing

1. Requirements

An L3 device networking topology need to be built to simulate the scenario, in which there are two interconnection links between the access devices and the core devices.

2. Topology

Figure 1-8 Topology for Configuring VLAN Load Balancing



3. Notes

- Configure instance mappings on switch D (switch E) to map VLAN 1 to instance 1, VLAN 2 to instance 2, VLAN 3 to instance 3, and VLAN 4 to instance 4. For details about how to configure the mappings, see "Configuring MSTP" in *Ethernet Switching Configuration Guide*.
- Configure the VLAN load balancing function on switch D (switch E).

4. Procedure

Perform the following configuration on switch D.

```
SwitchD> enable
SwitchD# configure terminal
SwitchD(config)# interface gigabitethernet 0/1
SwitchD(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchD(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2 prefer instance 2
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

Perform the following configuration on switch E.

```
SwitchE> enable
SwitchE# configure terminal
SwitchE(config)# interface gigabitethernet 0/1
SwitchE(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchD(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2 prefer instance 4
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

5. Verification

Run the **show interfaces switchport backup detail** command to check the dual-link backup information configured on switch D (switch E).

```
SwitchD# show interfaces switchport backup detail
Switch Backup Interface Pairs:
```

```
Active Interface        Backup Interface        State
------------------------------------------------------------------------------
Gi0/1                 Gi0/2                 Active Up/Backup Up

Instances Preferred on Active Interface: Instance 0-1,3-64
       Mapping VLAN 1,3-4094

Instances Preferred on Backup Interface: Instance 2
       Mapping VLAN 2

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : balance
Preemption Delay : 35 seconds
Bandwidth : Gi0/1(800 kbits), Gi0/2(100000 kbits)
```

```
SwitchE# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------------
Gi0/1                 Gi0/2                 Active Up/Backup Up

Instances Preferred on Active Interface: Instance 0-3,5-64
       Mapping VLAN 1-3,5-4094

Instances Preferred on Backup Interface: Instance 4
       Mapping VLAN 4

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : balance
Preemption Delay : 35 seconds
Bandwidth : Gi0/1(800 kbits), Gi0/2(100000 kbits)
```

6. Configuration Files

- Switch D configuration file

```
hostname SwitchD
!
interface GigabitEthernet 0/1
 switchport mode trunk
 switchport backup interface gigabitethernet 0/2 prefer instance 2
!

end
```

- Switch E configuration file

```
hostname SwitchE
!
```

```
interface GigabitEthernet 0/1
 switchport mode trunk
 switchport backup interface gigabitethernet 0/2 prefer instance 2
!

end
```

7. Common Errors

- The mappings between VLAN IDs and instances are not configured.

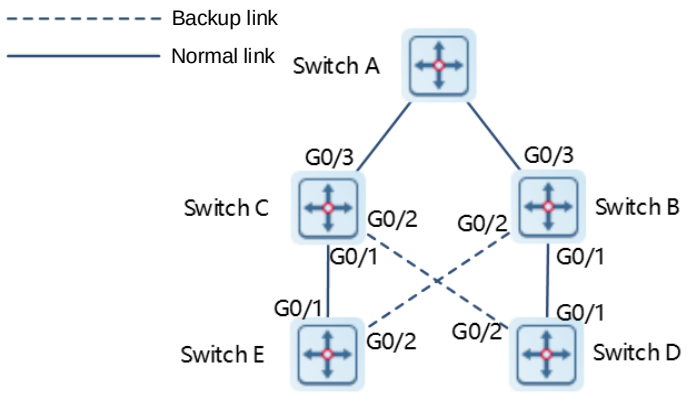
1.9.4 Configuring Link State Tracking

1. Requirements

An L3 device networking topology need to be built to simulate the scenario, in which there are two interconnection links between the access devices and the core devices.

2. Topology

Figure 1-9 Topology for Configuring Link State Tracking



3. Notes

- Create link state tracking group 1 on switch B (switch C).
- On switch B (switch C), add the ports GigabitEthernet 0/1 and GigabitEthernet 0/2 as downlink ports of the link state tracking group and add the port GigabitEthernet 0/3 as an uplink port of the link state tracking group.

4. Procedure

Perform the following configuration on switch B.

```
SwitchB> enable
SwitchB# configure terminal
SwitchB(config)# link state track 1
SwitchB(config)# interface GigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)# link state group 1 downstream
SwitchB(config-if-GigabitEthernet 0/1)# exit
```

```
SwitchB(config)# interface GigabitEthernet 0/2
SwitchB(config-if-GigabitEthernet 0/2)# link state group 1 downstream
SwitchB(config-if-GigabitEthernet 0/2)# exit
SwitchB(config)# interface GigabitEthernet 0/3
SwitchB(config-if-GigabitEthernet 0/3)# link state group 1 upstream
```

Perform the following configuration on switch C.

```
SwitchC> enable
SwitchC# configure terminal
SwitchC(config)# link state track 1
SwitchC(config)# interface GigabitEthernet 0/1
SwitchC(config-if-GigabitEthernet 0/1)# link state group 1 downstream
SwitchC(config-if-GigabitEthernet 0/1)# exit
SwitchC(config)# interface GigabitEthernet 0/2
SwitchC(config-if-GigabitEthernet 0/2)# link state group 1 downstream
SwitchC(config-if-GigabitEthernet 0/2)# exit
SwitchC(config)# interface GigabitEthernet 0/3
SwitchC(config-if-GigabitEthernet 0/3)# link state group 1 upstream
```

5. Verification

Run the **show link state group** command to check whether the configuration is correct.

```
SwitchB# show link state group
Link State Group:1  Status: enabled, Down
Upstream Interfaces :Gi0/3(Down)
Downstream Interfaces : Gi0/2(Down)

Link State Group:2  Status: Disabled, Down
Upstream Interfaces :
Downstream Interfaces :

(Up):Interface up   (Down):Interface Down   (Dis):Interface disabled
```

```
SwitchC# show link state group
Link State Group:1  Status: enabled, Down
Upstream Interfaces :Gi0/3(Down)
Downstream Interfaces : Gi0/2(Down)

Link State Group:2  Status: Disabled, Down
Upstream Interfaces :
Downstream Interfaces :

(Up):Interface up   (Down):Interface Down   (Dis):Interface disabled
```

6. Configuration Files

- Switch B configuration file

```
hostname SwitchB
```

```
!
link state track 1
interface GigabitEthernet 0/1
 link state group 1 downstream
!
interface GigabitEthernet 0/2
 link state group 1 downstream
!
interface GigabitEthernet 0/3
 link state group 1 upstream
!

end
```

- Switch C configuration file

```
hostname SwitchC
!
link state track 1
interface GigabitEthernet 0/1
 link state group 1 downstream
!
interface GigabitEthernet 0/2
 link state group 1 downstream
!
interface GigabitEthernet 0/3
 link state group 1 upstream
!

end
```

7. Common Errors

- Ports are added to a link state tracking group before the link state tracking group is enabled.

Contents

1 Configuring RLDP 1
1.1 Introduction 1
1.1.1 Basic Concepts 1
1.1.2 Detection Principles 3
1.1.3 RLDP Detection 4
1.2 Configuring Basic Features of RLDP 5
1.2.1 Overview 5
1.2.2 Restrictions and Guidelines 5
1.2.3 Procedure 6
1.3 Monitoring 6
1.4 Configuration Examples 7
1.4.1 Configuring Basic Features of RLDP 7
1.4.2 Configuring Unidirectional Link Detection 10
1.4.3 Configuring Bidirectional Link Detection 11

1 Configuring RLDP

1.1 Introduction

The Rapid Link Detection Protocol (RLDP) is an Ethernet link failure detection protocol, which is used to rapidly detect unidirectional link failures, bidirectional link failures, and downlink loop failures. When a failure is found, RLDP automatically shuts down relevant ports or asks users to manually shut down the ports according to the configured failure handling methods, to avoid wrong forwarding of traffic or Ethernet L2 loops.

1.1.1 Basic Concepts

1. Unidirectional Link Failure

A unidirectional link failure occurs when one end of the receiving or transmission link in an optical fiber is disconnected or not connected, one line in a twisted-pair cable is disconnected, or unidirectional disconnection occurs on an intermediate device between two devices. A unidirectional link failure can lead to wrong forwarding of traffic or the failure of a loop protection protocol such as Spanning Tree Protocol (STP).

2. Bidirectional Link Failure

A bidirectional link failure occurs when two optical fibers are disconnected, two lines in a twisted-pair cable are disconnected, or bidirectional disconnection occurs on an intermediate device between two devices. A bidirectional link failure can lead to the wrong forwarding of traffic.

3. Loop Failure

A loop failure occurs when a downlink port of a device is wrongly connected to another device and a loop forms. A loop failure can result in a broadcast storm.

4. Protocol Packets

RLDP defines the following three types of packets:

- Prob packets: L2 multicast packets used for neighbor negotiation, and unidirectional or bidirectional link detection. The default encapsulation format of the packets is of the Subnetwork Access Protocol (SNAP) type, which automatically changes to EthernetII if a neighbor sends EthernetII packets.
- Echo packets: L2 unicast packets in response to prob packets and used for unidirectional or bidirectional link detection. The default encapsulation format is of the SNAP type, which automatically changes to EthernetII if a neighbor sends EthernetII packets.
- Loop packets: L2 multicast packets for downlink loop detection. They can only be received by senders. The default encapsulation format of the packets is of the SNAP type.

5. Detection Interval

A detection interval and the maximum detection count can be configured for RLDP. A detection interval determines the period of sending prob packets and loop packets. When a device receives a prob packet, it replies with an echo packet immediately. A detection interval and the maximum detection count determine the maximum detection time (Detection interval × Maximum detection count + 1) for unidirectional or bidirectional link detection. If neither a prob nor an echo packet from a neighbor is correctly received within the maximum

detection time, the handling of unidirectional or bidirectional failures is triggered. The timers involved are described in Table 1-1.

Table 1-1 Description of RLDP Timers

Timer Name	Timer Description
Send timer	After the link detection function is enabled, the send timer is started and the prob packets or loop packets are sent regularly. The time interval of the send timer is the configured detection interval.
Timeout timer	● If a unidirectional or bidirectional link failure is detected, the timeout timer is started after the prob packet is sent, and the timeout time is the maximum detection time (Detection interval × Maximum detection count + 1). ● In unidirectional link detection, when the detection timeout time expires and a port can only receive the prob packet or response packet from the neighbor, it is considered that a unidirectional link failure occurs. ● In bidirectional link detection, when the detection timeout time expires and a port fails to receive the prob packet and response packet from the neighbor, it is considered that a bidirectional link failure occurs.

6. Neighbor Negotiation

When configured with unidirectional or bidirectional link detection, a port can learn a peer device as its neighbor. One port can learn only one neighbor, which is changeable. If the negotiation function is enabled, unidirectional or bidirectional link detection starts after a port finds a neighbor through negotiation. Negotiation is considered successful if the port receives a prob packet from the neighbor. However, if RLDP is enabled on a port after a failure already occurs, the port fails to learn a neighbor and detection fails to be started. In this case, you are advised to rectify the link failure first.

7. Associated Actions

The associated actions and recovery methods after a RLDP port failure are described in Table 1-2.

Table 1-2 Description of RLDP Port Failure Handling

Type	Associated Action/ Recovery Method	Description
Associated actions after a failure	warning	Only the relevant system log is printed to indicate the failed port and the failure type.
	Shutdown SVI	A system log is printed. If the failed port is a physical switching port or member port of an L2 aggregate port (AP), a switch virtual interface (SVI) is queried based on the access VLAN or native VLAN of the port, and then the SVI is shut down.
	Port errdisable	A system log is printed, the failed port is set in errdisable state, and the port enters the linkdown state physically.

Type	Associated Action/ Recovery Method	Description
	Block	A system log is printed, the forwarding state of the failed port is set to blocked, and the port does not forward received packets.
Recovery methods after a failure	Manual reset	Manually reset all the failed ports to the initialized state to restart link detection.
	Manual or automatic errdisable recovery	Recover all the failed ports to the initialized state manually or regularly (**30** seconds by default and configurable) and restart link detection.
	Automatic recovery	Under unidirectional or bidirectional link detection, if the handling method specified for failed ports does not enable the ports to enter the errdisable state, the ports can automatically recover to the initialized state based on prob packets exchanged with the neighbor, and link detection is restarted.
	Manual or automatic execution of the **rldp error-recover interval** command	All the failed ports recover to the initialized state regularly (configurable) and link detection is restarted.

8. RLDP Port State

RLDP ports can be in two states:

- Normal: Indicates the state of a port, on which link detection is enabled.
- Error: Indicates the state of a port, on which a unidirectional or bidirectional link failure or a loop failure is detected.

1.1.2 Detection Principles

A typical Ethernet link detection mechanism detects physical link connectivity through auto-negotiation at the physical layer. However, this detection mechanism has limitations. In some cases, devices are connected and work normally at the physical layer but L2 link communication fails or is abnormal. RLDP recognizes a neighbor device and detects whether a link failure exists by exchanging prob packets, echo packets, or loop packets with the neighbor device. Figure 1-1 shows the protocol states.

Figure 1-1 RLDP Protocol State Diagram

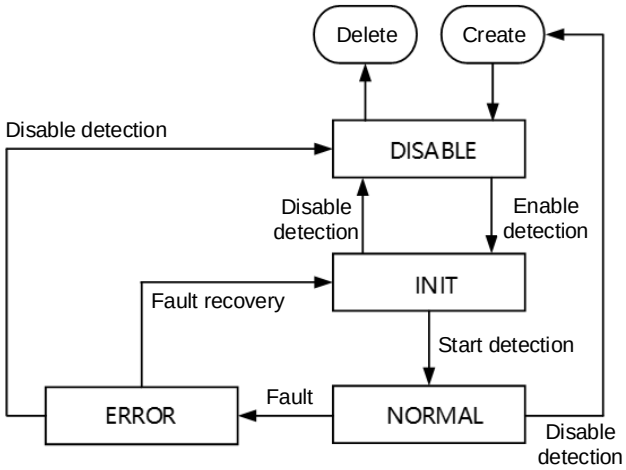


Figure 1-1 shows the detection logic of RLDP, which can be mainly in four states. The four states are described in Table 1-3.

Table 1-3 Description of RLDP States

State	Description
DISABLE	After the global RLDP function is enabled, all ports enter the disable state. Now, unidirectional link detection, bidirectional link detection, or downlink loop detection is not enabled on the ports. If the RLDP is disabled in any state, a port enters this state.
INIT	It refers to the initialized state after RLDP is just configured and enabled or a failure is rectified. Now, unidirectional link detection, bidirectional link detection, or downlink loop detection is enabled on ports, and the corresponding link failure handling methods are specified, or the links can recover from unidirectional failures, bidirectional failures, or loop failures automatically.
NORMAL	It refers to the state after detection is enabled for RLDP. For downlink loop detection, RLDP enters the state directly after enabled. For unidirectional or bidirectional link detection, RLDP enters the state directly or enters the state only after negotiation with a specified neighbor succeeds.
ERROR	It refers to the state after RLDP detects a failure. In this case, a unidirectional link failure or bidirectional link failure is detected on a port. The failure will be handled according to the specified failure handling method.

1.1.3 RLDP Detection

RLDP provides unidirectional link detection, bidirectional link detection, and downlink loop detection.

1. Unidirectional Link Detection

After unidirectional link detection is enabled, a port sends prob packets and receives echo packets from a neighbor regularly. It also receives prob packets from the neighbor and replies with echo packets to the

neighbor. If the port receives only prob packets but no echo packets, or none of them from the neighbor within the maximum detection time, handling of a unidirectional failure is triggered and the detection stops.

2. Bidirectional Link Detection

After bidirectional link detection is enabled, a port sends prob packets and receives echo packets from a neighbor regularly. It also receives prob packets from the neighbor and replies with echo packets to the neighbor. If the port receives neither prob packets nor echo packets from the neighbor within the maximum detection time, handling of a bidirectional failure is triggered and the detection stops.

3. Downlink Loop Detection

After downlink loop detection is enabled, a port sends loop packets regularly. After the same port or different ports on a device receive loop packets, a loop failure is triggered if any of the following cases occurs: The transmission and receiving ports of the packets are the same routed ports or L3 AP member ports; the transmission and receiving ports of packets are exchange ports or L2 AP member ports, the default VLANs of the ports are the same, and forwarding states of the ports are forward. The failure is handled according to the corresponding method and the detection stops.

1.2 Configuring Basic Features of RLDP

1.2.1 Overview

- You can enable RLDP unidirectional link detection, bidirectional link detection, or downlink loop detection to discover unidirectional, bidirectional, or loop failures.
- After global RLDP detection is enabled, the RLDP detection is started on each port normally.
- After the function is enabled in global configuration mode, RLDP detection on a port is started after successful neighbor negotiation.
- If loop detection latency interval is configured in global configuration mode, the downlink port loop cannot be detected in this period of time.
- In interface configuration mode, you can configure unidirectional RLDP detection, bidirectional RLDP detection, or downlink loop detection, and specify a failure handling method.
- You can restore all the failed ports and restart detection.

1.2.2 Restrictions and Guidelines

- Loop detection configured on an AP member port takes effect on all the member ports of the AP. Unidirectional link detection and bidirectional link detection take effect on an AP member port directly.
- The loop detection configuration of a physical port added to an AP must be the same as that of the other member ports of the AP. There are two cases. (1) If loop detection is not configured on the new member port but on the existing member ports, the new port adopts the configuration and detection results of the existing ports. (2) If the new member port and the existing member ports have different loop detection configurations, the new port adopts the configuration and detection results of the existing ports.
- When configuring the RLDP on an AP member port, you can configure only the "shutdown-port" and "warning" handling methods. If the failure handling method is not set to "shutdown-port" or "warning", it is modified to "shutdown-port" and takes effect.
- After the "shutdown-port" handling method is configured on a port, the port cannot resume RLDP detection

in the case of a failure. After confirming that the failure is rectified, you can run the **rldp reset** or **errdisable recovery** command to restore the port and restart detection. For the description and configuration of **errdisable recovery**, see "Configuring Ethernet Interface" in *Interface Configuration Guide*.

1.2.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the global RLDP detection function.

rldp enable

The global RLDP detection function is disabled by default.

(4) (Optional) Configure global neighbor negotiation.

rldp neighbor-negotiation

The neighbor negotiation function is disabled by default.

(5) (Optional) Configure the global RLDP detection interval.

rldp detect-interval *interval*

The default interval for sending RLDP packets by a port is **3** seconds.

(6) (Optional) Configure a time interval for RLDP to recover failed ports.

rldp error-recover interval *interval*

No time interval for RLDP to recover failed ports regularly is configured by default.

(7) (Optional) Configure the maximum detection count of RLDP.

rldp detect-max *max-detect-num*ber

The default maximum detection count of RLDP is **2**.

(8) (Optional) Configure the global loop detection latency interval.

rldp detect-latency *interval*

The default latency interval for global RLDP loop detection is **0** seconds.

(9) Enter the interface configuration mode.

interface *interface-type interface-number*

(10) Configure RLDP detection on the port.

rldp port { **bidirection-detect** | **loop-detect** | **unidirection-detect** } { **block** | **shutdown-port** | **shutdown-svi** | **warning** }

RLDP detection is not configured on a port by default.

1.3 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-4 RLDP Monitoring

Command	Purpose
show rldp [**interface** *interface-type interface-number*]	Displays the RLDP running state.

1.4 Configuration Examples

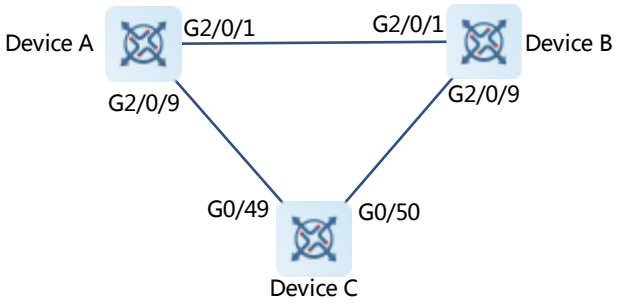
1.4.1 Configuring Basic Features of RLDP

1. Requirements

The aggregation and access devices form a ring topology. STP is enabled on all devices to prevent loops and provide redundancy protection. To avoid a unidirectional or bidirectional link failure resulting in an STP failure, RLDP unidirectional link detection and bidirectional link detection are enabled between aggregation devices as well as between the aggregation devices and the access device. To avoid loops due to wrong connection in the downlink direction of the aggregation devices, RLDP downlink loop detection is enabled on the downlink ports of the aggregation devices and the access device. To avoid loops due to wrong connection in the downlink direction of the access device, RLDP downlink loop detection is enabled on all the downlink ports of the access device.

2. Topology

Figure 1-2 Topology for Configuring Basic Features of RLDP



3. Notes

- Devices A and B are aggregation devices, and device C is an access device. User devices can be connected to downlink ports of device C. Devices A, B, and C are structured in a ring topology, and STP is enabled on each of them. For STP configuration, refer to the relevant configuration guide.
- Enable RLDP on device A, enable unidirectional and bidirectional link detection on the two ports, and enable loop detection on the downlink port.
- Enable RLDP on device B, enable unidirectional and bidirectional link detection on the two ports, and enable loop detection on the downlink port.
- Enable RLDP on device C, enable unidirectional and bidirectional link detection on the two uplink ports, and enable loop detection on the two downlink ports.

4. Procedure

Perform the following configuration on device A.

```
Device A# configure terminal
Device A(config)# rldp enable
Device A(config)# interface GigabitEthernet 2/0/1
Device A(config-if-GigabitEthernet 2/0/1)# rldp port unidirection-detect
shutdown-port
Device A(config-if-GigabitEthernet 2/0/1)# rldp port bidirection-detect shutdown-port
Device A(config-if-GigabitEthernet 2/0/1)# exit
Device A(config)# interface GigabitEthernet 2/0/9
Device A(config-if-GigabitEthernet 2/0/1)# rldp port unidirection-detect
shutdown-port
Device A(config-if-GigabitEthernet 2/0/1)# rldp port bidirection-detect shutdown-port
Device A(config-if-GigabitEthernet 2/0/1)# rldp port loop-detect shutdown-port
```

Perform the following configuration on device B.

```
Device B# configure terminal
Device B(config)# rldp enable
Device B(config)# interface GigabitEthernet 2/0/1
Device B(config-if-GigabitEthernet 2/0/1)# rldp port unidirection-detect
shutdown-port
Device B(config-if-GigabitEthernet 2/0/1)# rldp port bidirection-detect shutdown-port
Device B(config-if-GigabitEthernet 2/0/1)# exit
Device B(config)# interface GigabitEthernet 2/0/9
Device B(config-if-GigabitEthernet 2/0/1)# rldp port unidirection-detect
shutdown-port
Device B(config-if-GigabitEthernet 2/0/1)# rldp port bidirection-detect shutdown-port
Device B(config-if-GigabitEthernet 2/0/1)# rldp port loop-detect shutdown-port
```

Perform the following configuration on device C.

```
Device C# configure terminal
Device C(config)# rldp enable
Device C(config)# interface GigabitEthernet 0/49
Device C(config-if-GigabitEthernet 0/49)# rldp port unidirection-detect shutdown-port
Device C(config-if-GigabitEthernet 0/49)# rldp port bidirection-detect shutdown-port
Device C(config-if-GigabitEthernet 0/49)# exit
Device C(config)# interface GigabitEthernet 0/50
Device C(config-if-GigabitEthernet 0/50)# rldp port unidirection-detect shutdown-port
Device C(config-if-GigabitEthernet 0/50)# rldp port bidirection-detect shutdown-port
Device C(config-if-GigabitEthernet 0/50)# exit
Device C(config)# interface GigabitEthernet 0/1
Device C(config-if-GigabitEthernet 0/1)# rldp port loop-detect shutdown-port
Device C(config-if-GigabitEthernet 0/1)# exit
Device C(config)# interface GigabitEthernet 0/2
Device C(config-if-GigabitEthernet 0/2)# rldp port loop-detect shutdown-port
```

5. Verification

Check the RLDP state information on devices, A, B, and C. Device A is taken as an example. Run the **show rldp** command to check whether the configuration is correct.

```
Device A# show rldp
rldp state         : enable
rldp hello interval: 3
rldp max hello     : 2
rldp local bridge  : 00d0.f822.33aa
-----------------------------------
Interface GigabitEthernet 2/0/1
port state      : normal
neighbor bridge : 00d0.f800.51b1
neighbor port   : GigabitEthernet 2/0/1
unidirection detect information:
    action: shutdown-port
    state : normal
bidirection detect information:
    action: shutdown-port
    state : normal

Interface GigabitEthernet 2/0/9
port state      : normal
neighbor bridge : 00d0.f800.41b0
neighbor port   : GigabitEthernet 0/49
unidirection detect information:
    action: shutdown-port
    state : normal
bidirection detect information:
    action: shutdown-port
    state : normal
loop detect information:
    action: shutdown-port
    state : normal
```

6. Common Errors

- RLDP is enabled together with private multicast address authentication or TPP.
- Neighbor negotiation is not enabled when unidirectional or bidirectional link detection is configured. RLDP must be enabled on a neighbor device in global or interface configuration mode; otherwise a unidirectional or bidirectional failure is detected.
- If neighbor negotiation prior to RLDP detection is specified when unidirectional or bidirectional link detection is configured, normal detection fails because no neighbor is learned in the case of an existing link failure. In this situation, you are advised to rectify the link failure first.
- You are not advised to specify Shutdown SVI as the failure handling method on a routed port.
- You are not advised to specify Block as the failure handling method for a port, on which a loop protection

protocol such as STP is enabled.

1.4.2 Configuring Unidirectional Link Detection

1. Requirements

As shown in Figure 1-3, device A is connected to device B through an optical fiber. The two lines are the Tx and Rx lines of the optical fiber. Unidirectional link detection is enabled on devices A and B. If a fault occurs on either the Tx end of device A or Rx end of device B or on either the Rx end of device A or Tx end of device B, RLDP can detect the unidirectional failure and handle it. If the failure is eliminated, the administrator can manually restore the RLDP state on devices A and B and restart detection.

2. Topology

Figure 1-3 Topology for Configuring Unidirectional Link Detection

3. Notes

- Enable global RLDP.
- Configure unidirectional link detection of RLDP on ports and define a method for handling unidirectional failures.

4. Procedure

Perform the following configuration on device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# rldp enable
DeviceA(config)# interface GigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# rldp port unidirection-detect shutdown-port
```

Perform the following configuration on device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# rldp enable
DeviceB(config)# interface GigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# rldp port unidirection-detect shutdown-port
```

5. Verification

Check the RLDP state information on device A.

```
DeviceA> enable
DeviceA# show rldp
rldp state        : enable
rldp hello interval: 3
rldp max hello     : 2
```

```
rldp local bridge  : 00d0.f822.33aa
-----------------------------------
Interface GigabitEthernet 0/1
port state     : normal
neighbor bridge : 00d0.f800.51b1
neighbor port   : GigabitEthernet 0/1
unidirection detect information:
    action: shutdown-port
    state : normal
```

Check the RLDP state information on device B.

```
DeviceB> enable
DeviceB# show rldp
rldp state        : enable
rldp hello interval: 3
rldp max hello     : 2
rldp local bridge  : 00d0.f800.51b1
-----------------------------------
Interface GigabitEthernet 0/1
port state     : normal
neighbor bridge : 00d0.f822.33aa
neighbor port   : GigabitEthernet 0/1
unidirection detect information:
    action: shutdown-port
    state : normal
```

6. Common Errors

- Global RLDP is not enabled at the local end or peer end.
- The RLDP detection method configured at the local end is inconsistent with that at the peer end.
- RLDP negotiation is not enabled, so a link failure is judged by mistake when unidirectional link detection of RLDP is configured at a single end.

1.4.3 Configuring Bidirectional Link Detection

1. Requirements

As shown in Figure 1-4, device A is connected to device B through an optical fiber. The two lines are the Tx and Rx lines of the optical fiber. Bidirectional link detection is enabled on devices A and B. If a fault occurs on the Tx end of device A and Rx end of device B or on the Rx end of device A and Tx end of device B, RLDP can detect a bidirectional failure and handle it. If the failure is eliminated, the administrator can manually restore the RLDP state on devices A and B and restart detection.

2. Topology

Figure 1-4 Topology for Configuring Bidirectional Link Detection

3. Notes

- Enable global RLDP.
- Configure bidirectional link detection of RLDP on ports and define a method for handling bidirectional failures.

4. Procedure

Perform the following configuration on device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# rldp enable
DeviceA(config)# interface GigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# rldp port bidirection-detect shutdown-port
```

Perform the following configuration on device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# rldp enable
DeviceB(config)# interface GigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# rldp port bidirection-detect shutdown-port
```

5. Verification

Check the RLDP state information on device A.

```
DeviceA> enable
DeviceA# show rldp
rldp state        : enable
rldp hello interval: 3
rldp max hello     : 2
rldp local bridge  : 00d0.f822.33aa
-----------------------------------
Interface GigabitEthernet 0/1
port state      : normal
neighbor bridge : 00d0.f800.51b1
neighbor port   : GigabitEthernet 0/1
bidirection detect information:
    action: shutdown-port
    state : normal
```

Check the RLDP state information on device B.

```
DeviceB> enable
DeviceB# show rldp
rldp state        : enable
rldp hello interval: 3
rldp max hello    : 2
rldp local bridge  : 00d0.f800.51b1
-----------------------------------
Interface GigabitEthernet 0/1
port state     : normal
neighbor bridge : 00d0.f822.33aa
neighbor port   : GigabitEthernet 0/1
bidirection detect information:
    action: shutdown-port
    state : normal
```

6. Common Errors

- Global RLDP is not enabled at the local end or peer end.
- The RLDP detection method configured at the local end is inconsistent with that at the peer end.
- If bidirectional link detection needs to be configured but RLDP negotiation is not enabled, a link failure will be detected at one end.

Contents

1 Configuring DLDP 1
1.1 Introduction 1
1.1.1 Basic Concepts 1
1.1.2 DLDP Detection 2
1.1.3 MAC Address Binding 2
1.2 Configuring DLDP Detection 2
1.2.1 Overview 2
1.2.2 Restrictions and Guidelines 2
1.2.3 Procedure 3
1.3 Monitoring 3
1.4 Configuration Examples 4
1.4.1 Configuring DLDP Detection 4

1 Configuring DLDP

The Data Link Detection Protocol (DLDP) achieves rapid detection of Ethernet link failures. A typical Ethernet link detection mechanism detects physical link connectivity through auto-negotiation at the physical layer. However, such a mechanism has limitations in L3 data connectivity detection, for example, the physical connection is normal but L3 data communication is abnormal. DLDP provides reliable L3 link detection information. After detecting a faulty link, DLDP disables the logical function of L3 ports to realize fast L3 protocol convergence.

1.1 Introduction

1.1.1 Basic Concepts

1. Detection Mode

Active mode and passive mode are two DLDP detection modes.

- Active mode (default): In this mode, Internet Control Message Protocol (ICMP) detection packets are sent actively.
- Passive mode: In this mode, ICMP detection packets are received passively. Namely, DLDP returns an ICMP reply packet upon receiving an ICMP echo packet, instead of actively sending ICMP echo packets to the peer end. It judges whether an ICMP echo packet is received within a specified period to determine whether the link to the peer port is faulty. This mode not only implements the function of detecting link connectivity for the both devices, but also saves the bandwidth resources and device CPU resources.

2. Inter-Network Segment Detection

If DLDP needs to detect reachability to an IP address in a non-directly connected network segment, you need to configure the next-hop IP address for the local port so that DLDP can obtain the next-hop MAC address through an Address Resolution Protocol (ARP) packet, encapsulate an ICMP packet correctly, and send it out. In this situation, however, you need to avoid receiving an ICMP reply packet from another link; otherwise, DLDP misjudges that the port does not receive an ICMP reply.

3. Detection Time

When a network device does not receive a reply packet from the peer end within the period of the detection interval multiplied by the number of retransmission times, the device determines that an L link failure occurs and actively shuts down the logical function of its L3 port (despite the physical link reachable). Once the L3 link connectivity recovers, the device restores the logical function of the L3 port.

- Detection interval: Indicates the interval at which DLDP detection packets (ICMP echo) are transmitted.
- Retransmission times: Indicates the maximum number of times that DLDP detection packets can be retransmitted after a DLDP detection failure occurs.

4. Recovery Times

A detected link may be unstable, for example, the link can be pinged through only intermittently. The results of single DLDP detection are that the link is up/ down multiple times, which further destabilizes the ring network.

The term recovery times indicates the number of times that DLDP needs to receive reply packets consecutively before a link switches from the down state to up state. The default number of recovery times is 3, that is, a link can be pinged successfully three times before it is set to up. The recovery times configuration reduces link detection sensitivity but increases stability. Related parameters can be adjusted according to the network condition.

1.1.2 DLDP Detection

When detecting that an L3 link is abnormal, DLDP actively shuts down the L3 port. After the DLDP function is enabled, DLDP sends an ARP packet to obtain the MAC address and outbound port of the detected device or the next-hop device reachable to the detected device. Then DLDP periodically sends IPv4 ICMP echo packets to the MAC address and outbound port to detect link connectivity. If DLDP does not receive an IPv4 ICMP reply packet from the detected device within a specified period, DLDP determines that the link is abnormal and sets the L3 port to down. You can configure the next-hop IP address, MAC address of the detected device, transmission interval, number of retransmission times, and number of recovery times based on the actual environment to enable the DLDP detection function.

1.1.3 MAC Address Binding

In a complex network environment, DLDP may obtain an invalid MAC address if abnormal ARP packets are transmitted (due to ARP spoofing) in the detected link. As a result, DLDP fails to conduct detection normally. To address this problem, you can bind the to-be-detected IP address (or the next-hop IP address) to the MAC address of the device to avoid a DLDP failure caused by ARP spoofing. After binding, DLDP sends ARP packets and ICMP packets with a fixed destination IP address and a fixed destination MAC address during detection. If the source IP address and MAC address in a received packet do not match the bound IP address and MAC address, DLDP does not process the packet.

1.2 Configuring DLDP Detection

1.2.1 Overview

DLDP detects L3 link connectivity. When an L3 link is abnormal, DLDP shuts down the related L3 port.

1.2.2 Restrictions and Guidelines

- To configure the DLDP function, configure the next-hop IP address, MAC address, transmission interval, retransmission times, and recovery times based on the actual environment. You are not advised to set the number of retransmission times and the number of recovery times to 1. You are advised to use the default value for the transmission interval. The number of DLDP sessions and the configured CPU protect policy (CPP) bandwidth must be considered when you adjust the value. Otherwise, the device performance consumption increases and misjudgment and flapping can be caused easily. In the case of more than 10 sessions, the recommended interval is not smaller than 100 ticks.
- DLDP can detect multiple IP addresses configured on an L3 port. DLDP sets the port to down when none of the IP addresses returns an ICMP reply. If one of the IP addresses resumes communication, DLDP sets the port to up.
- DLDP uses the first IP address of the L3 port as the source IP address of detection packets.

1.2.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable DLDP detection.

dldp *ipv4-address* [*next-hop-ipv4-address*] [**mac-address** *mac-address*] [**interval** *tick-interval* | **resume** *resume-number* | **retry** *retry-number*]

By default, the number of retransmission times of DLDP detection is **4**, the number of recovery times is **3**, and the detection interval is **1** second.

(5) (Optional) Configure a DLDP detection mode.

dldp passive

The default DLDP detection mode is active mode.

(6) (Optional) Configure a global detection interval for DLDP detection.

dldp interval *tick-interval*

The default global detection interval of DLDP detection is **1** second.

The configuration of this command takes effect immediately for all DLDP detection operations.

(7) (Optional) Configure the number of global retransmission times for DLDP detection.

dldp retry *retry-number*

The default number of global retransmission times of DLDP detection is **4**.

The configuration of this command takes effect immediately for all DLDP detection operations.

(8) (Optional) Configure the number of link recovery times for all DLDP detection operations.

dldp resume *resume-number*

The default number of link recovery times of all DLDP detection operations is **3**.

The configuration of this command takes effect immediately for all DLDP detection operations.

1.3 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

Running the **clear** command during operation of the device may lose vital information and interrupt services.

Table 1-1 DLDP Monitoring

Command	Purpose
clear dldp [**interface** *interface-type interface-number* [*ipv4-address*]]	Clears the statistics on link up/down counts of a DLDP monitoring point.
show dldp [**interface** *interface-type interface-number*]	Displays the configuration of a DLDP monitoring point.
show dldp [**interface** *interface-type interface-number*] [**statistic**]	Displays the statistics of a DLDP monitoring point.

1.4 Configuration Examples

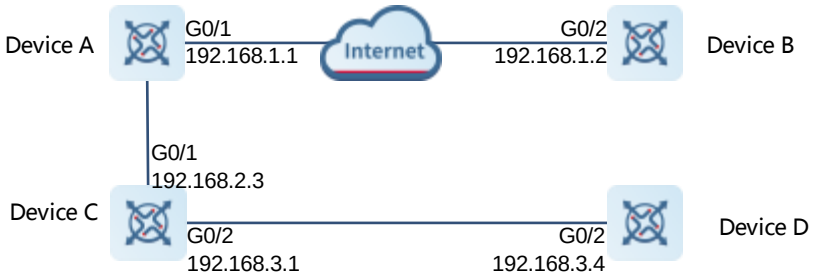
1.4.1 Configuring DLDP Detection

1. Requirements

DLDP detection needs to be enabled on an L3 network to control the L3 ports of devices A and B.

2. Topology

Figure 1-1 DLDP Topology



3. Notes

- Enable DLDP detection on the routed ports (GigabitEthernet 0/1 and GigabitEthernet 0/2) on device A to detect the L3 network connectivity from device A to device B and from device A to device D.
- To control the routed port (GigabitEthernet 0/2) of device B, enable DLDP detection and configure passive mode on the port.

4. Procedure

Perform the following configuration on device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# dldp 192.168.1.2
Device A(config-if-GigabitEthernet 0/1)# exit
```

```
Device A(config)# interface gigabitethernet 0/2
Device A(config-if-GigabitEthernet 0/2)# dldp 192.168.3.4 192.168.2.3
```

Perform the following configuration on device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface gigabitethernet 0/2
Device B(config-if-GigabitEthernet 0/2)# dldp 192.168.1.1
Device B(config-if-GigabitEthernet 0/2)# dldp passive
```

5. Verification

Run the **show dldp** command to check the DLDP state information on devices A and B and check whether DLDP detection is enabled and works normally.

```
Device A# show dldp
Interface  Type        Ip       Next-hop    Interval  Retry  Resume  State
---------  -------  -----------  -----------  --------  -----  ------  ------
Gi0/1     Active   192.168.1.2             100      4     3      Up
Gi0/1     Active   192.168.3.4  192.168.2.3  100      4     3      Up
```

```
Device B# show dldp
Interface  Type        Ip       Next-hop    Interval  Retry  Resume  State
---------  -------  -----------  -----------  --------  -----  ------  ------
Gi0/2     Passive  192.168.1.1             100      4     3      Up
```

6. Common Errors

- An unreachable IPv4 unicast route is misjudged as a DLDP detection failure.
- DLDP detection fails because the peer device does not support ARP/ICMP replies.
- No next-hop IP address is configured for inter-network segment DLDP detection.

Contents

1 Configuring VRRP 1
1.1 Introduction 1
1.1.1 Basic Concepts 1
1.1.2 VRRP Application 3
1.1.3 Packet Structure 5
1.1.4 VRRP State 8
1.1.5 VRRP Election 10
1.1.6 VRRP Timer 10
1.1.7 VRRP Tracking 11
1.1.8 Protocols and Standards 11
1.2 Restrictions and Guidelines 11
1.3 Configuration Task Summary 11
1.4 Configuring IPv4 VRRP 12
1.4.1 Overview 12
1.4.2 Restrictions and Guidelines 12
1.4.3 Procedure 12
1.5 Configuring IPv6 VRRP 13
1.5.1 Overview 13
1.5.2 Restrictions and Guidelines 13
1.5.3 Procedure 13
1.6 Configuring IPv4 VRRP Tracking 14
1.6.1 Overview 14

1.6.2 Restrictions and Guidelines 14

1.6.3 Procedure 15

1.7 Configuring IPv6 VRRP Tracking 15

1.7.1 Overview 15

1.7.2 Restrictions and Guidelines 15

1.7.3 Procedure 16

1.8 Configuring VRRP Attributes 17

1.8.1 Overview 17

1.8.2 Configuration Tasks 17

1.8.3 Configuring VRRP Basic Attributes 17

1.8.4 Configuring a Method of Sending IPv4 VRRP Packets on a Super VLAN Port 18

1.8.5 Configuring the Dual-Active Mode for an IPV4 VRRP Group 19

1.8.6 Configuring the IPv4 VRRP Packet Version 19

1.9 Monitoring 20

1.10 Configuration Examples 21

1.10.1 Configuring IPv4 VRRP 21

1.10.2 Configuring VRRP + MSTP 25

1 Configuring VRRP

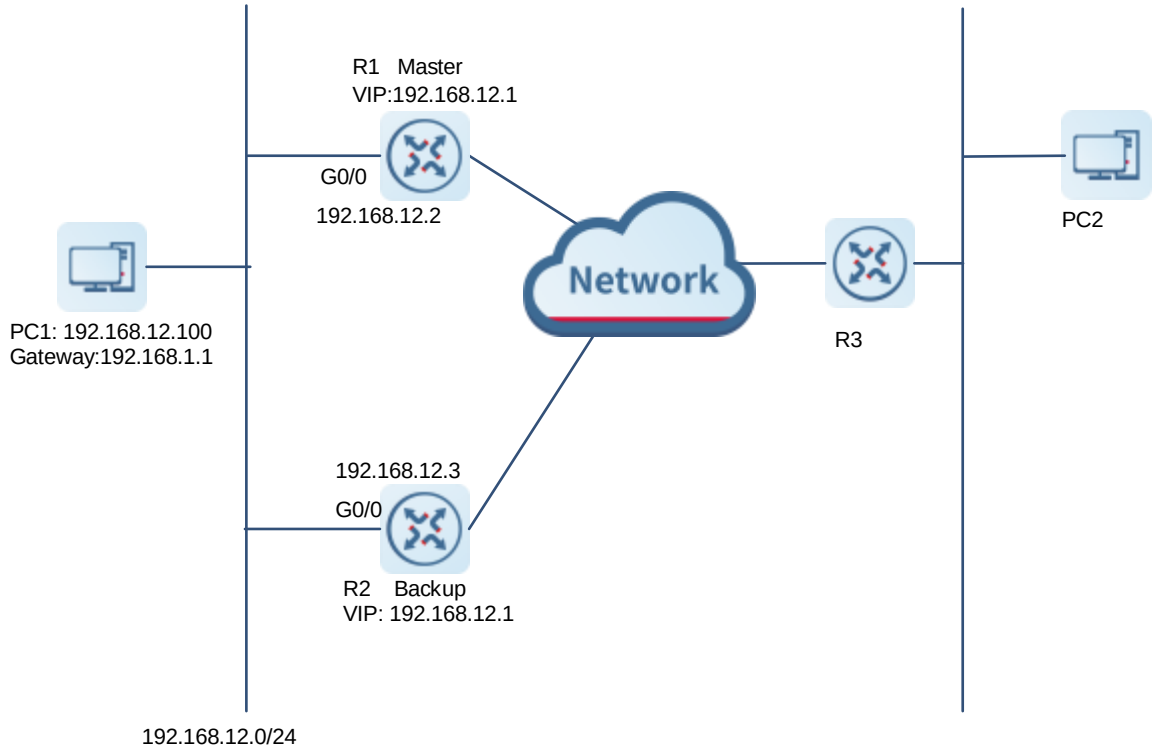
1.1 Introduction

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant routing protocol. When a device used for routing and forwarding on a local area network (LAN) fails, VRRP enables another device to automatically take over services and data of the device, which helps achieve hot backup and fault tolerance of IP routing. In addition, VRRP ensures communication continuity and reliability for the hosts on the LAN. VRRP is applicable to LAN scenarios which require redundant backup of routing egresses.

1.1.1 Basic Concepts

As shown in Figure 1-1, router 1 and router 2 form a VRRP backup group, and the gateway IP address configured for PC 1 is the virtual IP address of the VRRP backup group.

Figure 1-1 Diagram of Configuring VRRP



1. VRRP Router

A VRRP router refers to a router running VRRP. It is composed of one or more virtual routers.

2. Virtual Router

A virtual router, also called a VRRP backup group, is usually regarded as the default gateway of hosts on a shared LAN. A VRRP backup group contains a virtual router identifier (VRID) and a set of virtual IP addresses.

3. Master Router

In a VRRP backup group, only the master router responds to Address Resolution Protocol (ARP) requests and forwards IP packets. If a device is the IP address owner, it becomes the master router.

4. Backup Router

In a VRRP backup group, a backup router only monitors the state of the master router but does not respond to ARP requests or forward IP packets. When the master router fails, the backup router takes the chance to become the master router via election.

5. VRID

A virtual router identifier (VRID) is the unique identifier of a virtual router and distinguishes different VRRP back groups. Only a group of routers with the same VRID can form a VRRP backup group.

6. Priority

A VRRP backup group determines the position of each router in the virtual router based on its priority. The configurable priority range is from 1 to 254, and the priority of the VRRP router with the virtual router IP address must be 255. When the priority is 0, the current master node no longer joins the VRRP backup group, and the backup router is triggered to become the master node rapidly without waiting for the current master node to time out.

7. Virtual IP Address

A virtual IP address is the IP address of a virtual router. A virtual router can be configured with one or multiple virtual IP addresses.

8. Virtual MAC Address

A virtual MAC address of VRRP complies with the Request for Comments (RFC) protocol standard. The virtual MAC address of an IPv4 VRRP backup group is "00-00-5E-00-01-{VRID}" (the virtual MAC address of an IPv6 VRRP backup group is “00-00-5E-00-02-{VRID}”), with the first five bytes fixed and the last byte of a VRRP backup group ID. A VRRP backup group responds to an ARP request by using its virtual MAC address instead of the real MAC address of an interface.

9. IP Address Owner

If the virtual IPv4/IPv6 address of a VRRP backup group is consistent with the IPv4/IPv6 address of the Ethernet port on which the VRRP backup group is configured, that is, the VRRP backup group has the real IP address of the Ethernet port, the VRRP backup group is collectively called an IP address owner. In such a case, the priority of the VRRP backup group is 255. If the Ethernet port is available, the VRRP backup group enters the master state automatically. The IP address owner receives and processes the packets whose destination IP address is the IP address of the virtual router.

10. Preemption Mode

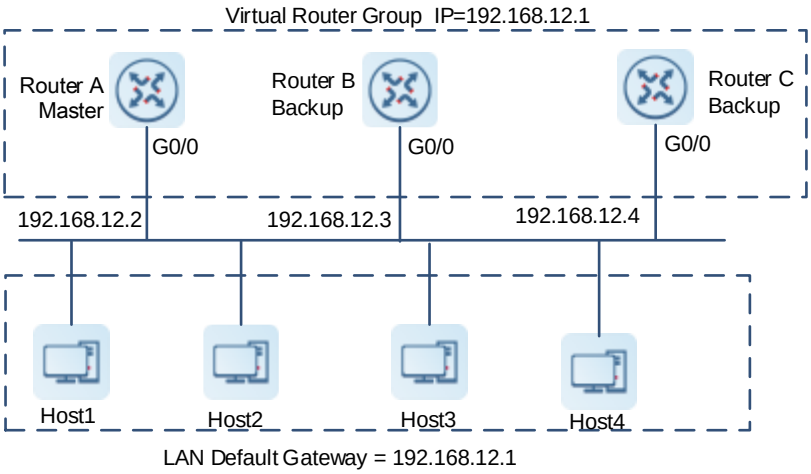
If a VRRP backup group runs in preemption mode, a backup router with a higher priority replaces the master router with a lower priority to become the master router of the VRRP backup group. If the VRRP backup group runs in the non-preemption mode, as long as the master router runs properly, the backup router does not become the master router even if it is configured with a higher priority later. In some cases, even if the non-preemption mode is configured, a router that is just started in a VRRP backup group will preempt the

position of the VRRP master router. The reason is that, when a device is started or the port just becomes active, the VRRP backup group on the port fails to receive the VRRP packet sent by the master device of the same backup group in time. In this case, the above problem can be avoided by delaying the start of the VRRP backup group.

1.1.2 VRRP Application

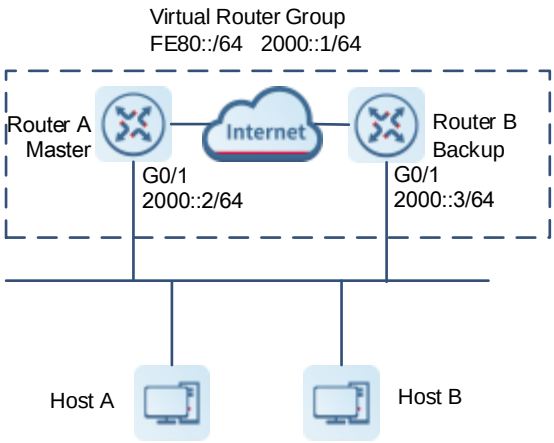
1. Master/Backup Redundancy

Figure 1-2 IPv4-based VRRP Master/Backup Redundancy



As shown in Figure 1-2, routers A, B, and C are all connected to the LAN through Ethernet ports, and VRRP is configured on the Ethernet ports connected to the LAN. The routers are in the same VRRP backup group, and the virtual IP address of the VRRP backup group is 192.168.12.1. Router A is elected as the master router of the VRRP backup group, and routers B and C are used as backup routers. Hosts 1, 2 and 3 use the IP address of the virtual router 192.168.12.1 as the gateway address. Packets from a host on the LAN to other networks are forwarded by the master router (router A). If router A fails, a master router is reelected between router B and router C to forward packets, to achieve simple routing redundancy.

Figure 1-3 IPv6-based VRRP Master/Backup Redundancy

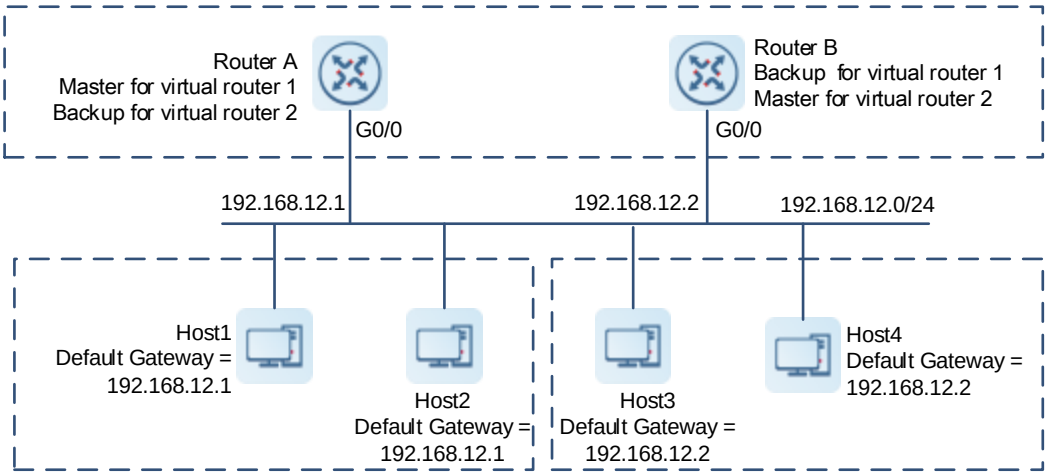


As shown in Figure 1-3, both routers A and B are connected to the LAN through Ethernet ports, and IPv6 VRRP is configured on the Ethernet ports connected to the LAN. The routers are in the same IPv6 VRRP backup group, and the virtual IPv6 addresses of the IPv6 VRRP backup group are FE80::1/64 and 2000::1/64. Router A is elected as the master router of VRRP, and router B functions as a backup router. The hosts on the LAN take the IPv6 link local address FE80::1/64 of the virtual router as the gateway address. Packets from the hosts on the LAN to other networks are forwarded by the master router. If router A fails, router B forwards packets on behalf of router A, achieving simple routing redundancy.

- Before implementation: If the uplink or downlink port of router A fails, the data flow is interrupted, that is, a single point of failure occurs.
- After implementation: If router A fails, VRRP implements switching within seconds to ensure that services are not interrupted. This effectively avoids the problem of network interruption after a single link fails. In addition, you do not need to modify the configuration such as the dynamic routing protocol and routing discovery protocol. You do not need to modify the default gateway configuration for the host node of local link.

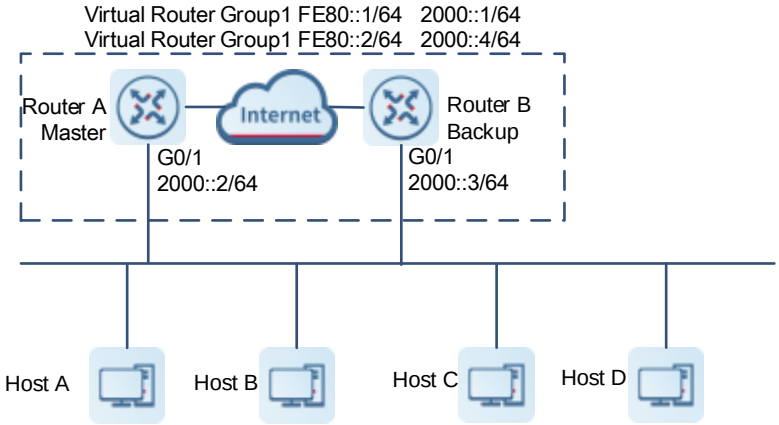
2. Load Balancing

Figure 1-4 IPv4-based VRRP Load Balancing



As shown in Figure 1-4, two virtual routers are configured. For virtual router 1, router A uses the IP address 192.168.12.1 of the Ethernet port GigabitEthernet 0/0 as the IP address of the virtual router, so router A becomes the master router and router B becomes the backup router. For virtual router 2, router B takes the IP address 192.168.12.2 of Ethernet port GigabitEthernet 0/0 as the IP address of the virtual router, so router B becomes the master router and router A becomes the backup router. In the LAN, hosts 1 and 2 take the IP address 192.168.12.1 of virtual router 1 as the default gateway address, while hosts 3 and 4 take the IP address 192.168.12.2 of virtual router 2 as the default gateway address. In this application of VRRP, routing redundancy is achieved between routers A and B, and the LAN traffic is shared between them to achieve load balancing.

Figure 1-5 IPv6-based VRRP Load Balancing



As shown in Figure 1-5, two virtual routers are configured. For virtual router 1, router A uses the IP address fe80::1/64 of the Ethernet port GigabitEthernet 0/1 as the IP address of the virtual router, so router A becomes the master router and router B becomes the backup router. For virtual router 2, router B takes the IP address fe80::2/64 of Ethernet port GigabitEthernet 0/1 as the IP address of the virtual router, so router B becomes the master router and router A becomes the backup router. On the LAN, hosts A and B use the IP address FE80::1 of virtual router 1 as the default gateway address (manually configured static IPv6 gateway), and hosts C and D use the IP address FE80::2 of virtual router 2 as the default gateway address (manually static configured IPv6 gateway). In this way, routing redundancy is achieved between routers A and B, and the LAN traffic is shared between them to achieve load balancing.

The devices involved are L3 devices or routers. L2 devices are not applicable.

- Before implementation: All traffic goes through the master router, causing a certain burden to the master router. Before the master router fails, the backup router has been always idle, leading to a resource waste.
- After implementation: Each device is not a single master router or backup router, but acts as different roles in different groups. Therefore, the connected devices can be assigned to different groups and forward traffic to different gateways to achieve traffic load balancing. Moreover, no device is kept idle all the time, and resources are fully utilized.

1.1.3 Packet Structure

VRRP has two versions available: VRRPv2 and VRRPv3. VRRPv2 is only applicable to IPv4 networks, and VRRPv3 is applicable to both IPv4 and IPv6 networks. A VRRP packet is used to send the priority and state of the master device to all backup devices in the same backup group in multicast mode (with the destination address 224.0.0.18). The packet is encapsulated in an IP packet. The source address is the primary IP address (not the virtual IP address) of the packet sending port, the time to live (TTL) is 255, and the protocol ID is 112. Figure 1-6 and Figure 1-7 show the structures of VRRPv2 and VRRPv3 packets respectively.

Figure 1-6 Structure of VRRPv2 Packets

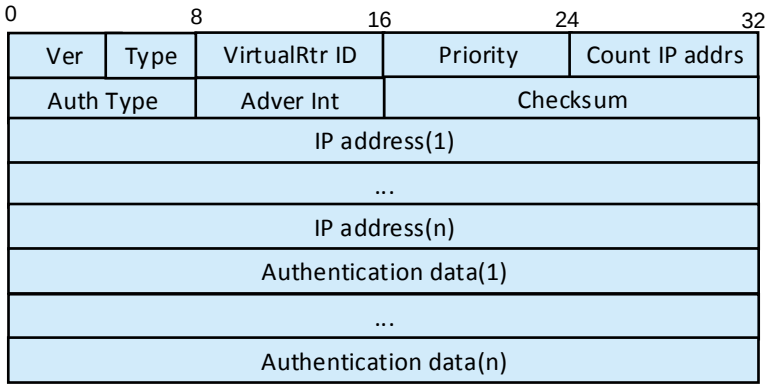


Figure 1-7 Structure of VRRPv3 Packets

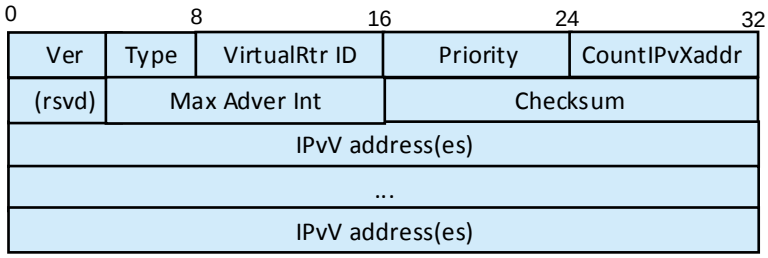


Table 1-1 Fields of VRRP Packets and Description

Packet Field	Description	
	VRRPv2	**VRRPv3**
Ver	Protocol version number. The value is 2.	Protocol version number. The value is 3.
Type	VRRP packet type. The value is 1, indicating that only the advertisement packets of VRRP are supported.	VRRP packet type. The value is 1, indicating that only the advertisement packets of VRRP are supported.
Virtual Rtr ID (VRID)	Virtual router ID (also the backup group ID). The value range is from 1 to 255.	Virtual router ID (also the backup group ID). The value range is from 1 to 255.

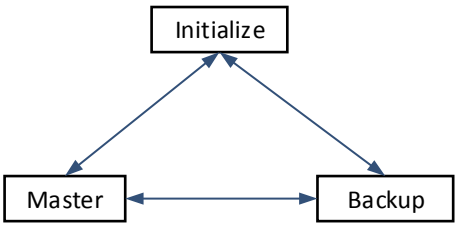
Packet Field	Description	
	VRRPv2	**VRRPv3**
Priority	Priority of the router in the backup group. The value range is from 0 to 255, and the default value is **100**. A larger value indicates a higher priority. When the priority is 0, the current master node no longer joins the VRRP backup group and the backup router is triggered to become the master node, instead of waiting for the current master node to time out. The priority 255 is reserved for the IP address owner, and the configurable range is from 1 to 254 for other routers.	Priority of the router in the backup group. The value range is from 0 to 255, and the default value is **100**. A larger value indicates a higher priority. When the priority is 0, the current master node no longer joins the VRRP backup group and the backup router is triggered to become the master node, instead of waiting for the current master node to time out. The priority 255 is reserved for the IP address owner, and the configurable range is from 1 to 254 for other routers.
Count IP Addrs/Count IPvX Addr	Number of virtual IPv4 addresses in the backup group.	Number of virtual IPv4 or virtual IPv6 addresses in the backup group.
Auth Type	Authentication type. Three authentication types are defined: ● **0**: Indicates no authentication. ● **1**: Indicates simple password (plaintext) authentication. ● **2**: Indicates MD5 authentication.	-
Advertise Interval	Interval of sending advertisement packets, in seconds. The default value is **1** second.	Interval of sending advertisement packets, in centiseconds. The default value is **100** centiseconds, namely, **1** second.
Checksum	16-bit checksum, used to check data corruption in the VRRP packet.	16-bit checksum, used to check data corruption in the VRRP packet.
IP Address/IPvX Address(es)	Virtual IPv4 addresses in the backup group. The number of addresses contained is defined in the **Count IP Addrs** field.	Virtual IPv4 addresses or virtual IPv6 addresses in the VRRP backup group. The number of addresses contained is defined in the **Count IPvX Addrs** field.

Packet Field	Description	
	VRRPv2	VRRPv3
Authentication Data	Authentication key of the VRRP packet. At present, the authentication key is only used for simple password authentication. For the other authentication methods, **0** is filled in this field.	-
rsvd	-	Reserved field for the VRRP packet. The field must be set to **0**.

1.1.4 VRRP State

There are three VRRP states: initialize, backup, and master. Figure 1-8 shows the state transition process.

Figure 1-8 VRRP State Transition Diagram



1. Initialize

Initialize is the initial state of VRRP. The system enters this state after startup. It only responds to startup, that is, it does not process VRRP packets.

- When the system is started, if the priority of the local VRRP backup group is 255 (namely, the IP address owner), then:
  - VRRP packets are sent immediately.
  - If the local VRRP backup group is an IPv4 virtual router, gratuitous ARP packets are sent to all the IPv4 addresses of the virtual router. If the local VRRP backup group is an IPv6 virtual router, gratuitous NA packets are sent to all the IPv6 addresses of the virtual router, the routing flag bit is 1, the request flag bit is 0, the coverage flag bit is 1, the target address is the IPv6 address of the virtual router (not destination address), and the link layer address in the target link layer option is the MAC address of the virtual router.
  - The advertisement information timer is configured to send VRRP advertisements regularly, that is, **Adver_Timer** is set to **Advertisement_Interval**.
  - The local VRRP backup group switches to the master state.
- When the system is started, if the priority of the local VRRP backup group is not 255, then:
  - **Master_Adver_Interval** is set to **Advertisement_Interval**.

- **Master_Down_Timer** is set to **Master_Down_Interval**.
- The local VRRP backup group switches to the backup state.

2. Backup

A backup virtual router is used to monitor the validity and state of the master virtual router.

- An IPv4 backup virtual router does not respond to the ARP request for the IP address of the virtual router, and an IPv6 backup virtual router does not respond to the neighbor solicitation (NS) packet for the IPv6 address of the virtual router.
- The backup virtual router discards packets whose destination MAC addresses are the MAC address of the VRRP backup group and packets whose destination IP addresses are the IP address of the VRRP backup group.
- The backup virtual router does not send protocol packets. It must receive the VRRP multicast packets sent by the master router to know the state of the master router.
- When a shutdown event is received, the backup virtual router deletes the host timeout timer and switches to the initialize state.
- If a timeout event of the host timeout timer is received, the backup virtual router sends VRRP advertisement information immediately. If the backup virtual router is an IPv4 virtual router, it broadcasts ARP packets to all the IPv4 addresses of the virtual router. If the backup virtual router is an IPv6 virtual router, it computes and joins the solicited-node multicast address for the IPv6 address associated with the virtual router, and sends non-request (gratuitous) NA packets to all the IPv6 addresses of the virtual router. The routing flag bit is 1, the request flag bit is 0, the coverage flag bit is 1, the target address is the IPv6 address of the virtual router (not destination address), and the link layer address in the target link layer option is the MAC address of the virtual router. **Adver_Timer** is set to **Advertisement_Interval**, and the virtual router switches to the master state.
- If a VRRP packet is received and the priority is 0, the host timeout timer **Master_Down_Timer** is reset to **Skew_Time**; if the priority of the received VRRP packet is greater than 0, and preemption is not allowed or the priority of the packet is greater than or equal to the priority of the local virtual router, **Adver Interval** is set to the **Master_Adver_Interval** field value in the packet and **Master_Down_Interval** is set to **Master_Down_Timer**, otherwise the packet is discarded.

3. Master

As the forwarding role in a VRRP backup group, the virtual router in the master state forwards virtual gateway packets.

- It sends VRRP multicast packets regularly, and forwards relevant packets passing through the virtual IP address and packets whose destination MAC address is the VRRP virtual MAC address.
- If the virtual router is an IPv4 virtual router, the VRRP virtual MAC address must be used to respond to the ARP requests whose destination IP addresses are the virtual IP address of the virtual router. If the virtual router is an IPv6 virtual router, it must respond to the NS packets whose destination IP addresses are the virtual IPv6 address of the virtual router and must be a member of the solicited-node multicast address for the IPv6 address associated with the virtual router.
- If **Accept_Mode** or **IPvX Owner** is configured, that is, the virtual router is the IPv4/IPv6 address owner, the packets whose destination IP addresses are the virtual IP address of the virtual router must be received, otherwise the packets are discarded.

- When the network port where the VRRP virtual router is located receives a shutdown event, the virtual router deletes the regular advertisement timer, removes the value of **Adver_Timer**, immediately sends a VRRP advertisement packet with priority 0, and switches to the initialize state.
- If the timer for sending VRRP packets times out or a VRRP packet with priority 0 is received, the VRRP advertisement message is sent immediately, the timer for sending VRRP packets is reset, and **Adver_Timer** is assigned to **Advertisement_Interval**.
- If the priority of the received VRRP packet is greater than or equal to that of the corresponding VRRP virtual router at the local end and the source IP address of the received packet is greater than the primary IP address at the local end, the host timeout timer is reset, the regular advertisement timer is configured, and the virtual router switches to the backup state.
- If none of the above requirements is met, the packets are discarded.

1.1.5 VRRP Election

VRRP provides a simple mechanism for electing the master router, which provides the actual routing and forwarding service. The master router is elected in the following order:

(1) VRRP judges whether the VRRP device is an IP address owner. If so, VRRP switches to the master state.

(2) VRRP judges the VRRP priority in the same VRRP backup group. The device with a larger priority is in the master state.

(3) VRRP judges the primary IP address of the network port. The device with a larger primary IP address changes to the master state.

(4) The backup device determines whether to switch the state by monitoring the VRRP packet regularly sent by the master device. It switches the state in the following two cases:

  - If the received advertisement state of the master device is normal, the priority of the master device's advertisement is lower than that of the backup device, and the preemption mode has been configured, the backup device switches to the master state.
  - If no state advertisement is received from the master device within the timeout period and the preemption mode is configured, the backup device switches to the master state.

1.1.6 VRRP Timer

The main VRRP timers include the VRRP advertisement sending interval timer and the VRRP preemption delay timer.

- VRRP advertisement sending interval timer

You can adjust the time interval for the master router to send VRRP advertisement packets by configuring the VRRP advertisement sending interval timer. If the backup router still fails to receive a VRRP advertisement packet after waiting for at least three intervals, it regards itself as the master router, and sends a VRRP advertisement packet to reelect the master router.

- VRRP preemption delay timer

To avoid frequent master/backup switching between the members of the backup group and allow the backup router to have enough time to collect necessary information (such as the routing information), the backup router does not immediately preempt the position of the master router after receiving the advertisement packet with a priority lower than the local priority, but waits for a period of time (preemption delay) before sending a VRRP advertisement packet to take the place of the original master router.

1.1.7 VRRP Tracking

By correlating with the tracking function, VRRP monitors port state changes and the IP host accessibility and automatically adjusts the priority of the backup group to trigger role competition in the backup group, which causes state switching in the backup group and achieves fault monitoring and automatic switching. In this way, the network traffic is not interrupted. Two detection methods are available:

- Port state: VRRP detects the port state by receiving port state change messages. When a port is no longer in the up state, the priority of the current master router is automatically reduced to enable other backup routers to have the opportunity to become the master router. This avoids the failure of the entire virtual router due to the disconnection of a certain line.
- Host accessibility: Internet Control Message Protocol (ICMP) detection packets are sent regularly, and the time interval for sending detection packets, timeout time for waiting for responses, and continuous timeout count are configured to judge accessibility of the destination addresses.

Caution

- A monitored port must be a routable L3 logical port (for example, a routed port, an SVI, a loopback port, or a tunnel port). If a VRRP backup group is an IPv6 group, the IPv6 function needs to be enabled on the port first.
- The decrease in the priority value must be greater than the priority difference between the master and backup devices; otherwise the priority of the master device may be the same as that of the backup device after priority adjustment, and the master/backup state cannot be switched.

1.1.8 Protocols and Standards

- RFC2338: Virtual Router Redundancy Protocol
- RFC3768: Virtual Router Redundancy Protocol (VRRP)
- RFC5798: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6

1.2 Restrictions and Guidelines

- The IPv6 VRRP and IPv4 VRRP backup groups share the VRRP backup group ID. One VRRP backup group ID is applicable to an IPv4 VRRP backup group and an IPv6 VRRP backup group configured on the same port.
- When the IPv4 VRRP and IPv6 VRRP backup groups of the same port use the same VRRP backup group ID, two VRRP backup group IDs are used.

1.3 Configuration Task Summary

VRRP configuration includes the following tasks:

(1) Configuring IPv4 VRRP

(2) Configuring IPv6 VRRP

(3) Configuring IPv4 VRRP Tracking

(4) Configuring IPv6 VRRP Tracking

(5) (Optional) Configuring VRRP Attributes

All the following configuration tasks are optional and may be selected as needed.

- Configuring VRRP Basic Attributes
- Configuring a Method of Sending IPv4 VRRP Packets on a Super VLAN Port
- Configuring the Dual-Active Mode for an IPV4 VRRP Group
- Configuring the IPv4 VRRP Packet Version

1.4 Configuring IPv4 VRRP

1.4.1 Overview

IPv4 VRRP creates a backup group on a specified LAN segment after the backup group ID and virtual IPv4 address are configured, and then the VRRP single backup function is enabled on the corresponding port. You can configure multiple VRRP backup groups on the same Ethernet port to achieve load balancing and offer more stable and reliable network services through mutual backup.

1.4.2 Restrictions and Guidelines

- To achieve VRRP, the routers in a VRRP backup group must be configured with the same virtual IPv4 address.
- To achieve mutual backup between multiple IPv4 VRRP backup groups, configure multiple same IPv4 VRRP backup groups with different priorities on ports so that they act as the master and backup groups mutually.
- Enable VRRP on L3 ports.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L3 interface configuration mode.

interface *interface-type interface-number*

(4) Enable IPv4 VRRP.

vrrp *group-id* **ip** *ipv4-address* [**secondary**]

IPv4 VRRP is disabled on a port by default.

(5) Configure a priority for the IPv4 VRRP backup group.

vrrp *group-id* **priority** *priority*

The default priority of an IPv4 VRRP backup group is **100**.

(6) (Optional) Configure a VRRP packet standard for the IPv4 VRRP backup group.

vrrp *group-id* **version** { **2** | **3** }

IPv4 VRRP adopts the VRRPv2 standard by default.

(7) (Optional) Configure an authentication string for the IPv4 VRRP backup group.

vrrp *group-id* **authentication** *authentication-string*

No authentication string of IPv4 VRRP is configured by default.

(8) (Optional) Configure a name for the IPv4 VRRP backup group.

vrrp *group-id* **description** *group-name*

No VRRP group name is configured by default.

(9) (Optional) Configure a VRRP advertisement interval for the IPv4 VRRP master router.

vrrp *group-id* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

The default VRRP advertisement interval of the VRRP master router is **1** second.

(10) (Optional) Enable the IPv4 VRRP timer learning function.

vrrp *group-id* **timers learn**

The advertisement interval timer learning function is disabled for an IPv4 VRRP backup group by default.

(11) (Optional) Configure the preemption mode for the IPv4 VRRP backup group.

vrrp *group-id* **preempt** [**delay** *delay-seconds*]

IPv4 VRRP runs in the preemption mode without preemption delay by default.

(12) (Optional) Configure a startup delay for the VRRP backup group on the port.

vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }

No VRRP group startup delay is configured by default.

1.5 Configuring IPv6 VRRP

1.5.1 Overview

IPv6 VRRP creates a backup group on a specified LAN segment after the backup group ID and virtual IPv6 address are configured, and then the VRRP single backup function is enabled on the corresponding port. You can configure multiple VRRP backup groups on the same Ethernet port to achieve load balancing and offer more stable and reliable network services through mutual backup.

1.5.2 Restrictions and Guidelines

- The first configured virtual address for IPv6 VRRP must be a link-local address, which can be deleted only after other virtual addresses are deleted.
- The IPv6 function must be enabled on a port before IPv6 VRRP is configured.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L3 interface configuration mode.

interface *interface-type interface-number*

(4) Enable the IPv6 function on the port.

ipv6 enable

(5) Enable IPv6 VRRP.

vrrp *group-id* **ipv6** *ipv6-address*

IPv6 VRRP is disabled on a port by default.

(6) Enable the function of receiving packets whose destination addresses are the IPv6 address of the virtual router.

vrrp ipv6 accept_mode

By default, an IPv6 VRRP group in the master state is not permitted to receive packets whose destination addresses are the IPv6 address of a virtual router, except the IPv6 VRRP group in owner state or the received NA/NS packets.

(7) Configure a priority for the IPv6 VRRP backup group.

vrrp ipv6 *group-id* **priority** *priority*

The default priority of an IPv6 VRRP backup group is **100**.

(8) (Optional) Configure a name for the IPv6 VRRP backup group.

vrrp ipv6 *group-id* **description** *group-name*

No VRRP group name is configured by default.

(9) (Optional) Configure a VRRP advertisement interval for the IPv6 VRRP master router.

vrrp ipv6 *group-id* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

The default VRRP advertisement interval of the VRRP master router is **1** second.

(10) (Optional) Enable the IPv6 VRRP timer learning function.

vrrp ipv6 *group-id* **timers learn**

The advertisement interval timer learning function is disabled for an IPv6 VRRP group by default.

(11) (Optional) Configure the preemption mode for the IPv6 VRRP backup group.

vrrp ipv6 *group-id* **preempt** [**delay** *delay-seconds*]

IPv6 VRRP runs in the preemption mode without preemption delay by default.

1.6 Configuring IPv4 VRRP Tracking

1.6.1 Overview

IPv4 VRRP tracking monitors the changes in port state and the IPv4 host accessibility. You can configure the optional packet detection parameter and bidirectional forwarding detection (BFD) correlation. The priority of a backup group can be adjusted dynamically to implement automatic switching and recovery of the backup group in case of a failure monitored.

1.6.2 Restrictions and Guidelines

- A monitored port must be a routable L3 logical port (for example, a routed port, an SVI, a loopback port, or a tunnel port).
- If a VRRP group uses the actual IP address of an Ethernet port (in the owner state), the group priority is 255, and the monitored IP address or port can be configured, but the priority of the VRRP group is not changed.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a port to be monitored by an IPv4 VRRP backup group.

vrrp *group-id* **track** { *interface-type interface-number* | **bfd** *interface-type interface-number ipv4-address* } [*priority*]

No port to be monitored by an IPv4 VRRP backup group is configured by default. If a port to be monitored by an IPv4 VRRP backup group is configured and the priority parameter is not specified, the priority change value is 10.

(5) Configure an IP address to be monitored by the IPv4 VRRP backup group.

vrrp *group-id* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

No IP address to be monitored by an IPv4 VRRP backup group is configured by default. If an IP address to be monitored by an IPv6 VRRP group is configured, the time interval for sending detection packets is 3 seconds, and the timeout time for waiting for a response to a sent detection packet is 1 second, and the consecutive timeout count for judging that a tracked IP address is unreachable is 3.

(6) Configure BFD correlation with the IPv4 VRRP group.

vrrp *group-id* **bfd** *ip-address*

BFD correlation with an IPv4 VRRP group is not configured on a port by default.

(7) Return to the global configuration mode.

exit

(8) Configure global IPv4 VRRP BFD.

vrrp bfd *interface-type interface-number ip-address*

By default, no global BFD mode is configured for IPv4 VRRP to detect whether the master device is active.

1.7 Configuring IPv6 VRRP Tracking

1.7.1 Overview

IPv6 VRRP tracking monitors the changes in port state and the IPv6 host accessibility. You can configure the optional packet detection parameter to dynamically adjust the priority of a backup group and implement automatic switching and recovery of the backup group in case of a failure monitored.

1.7.2 Restrictions and Guidelines

- A monitored port must be a routable L3 logical port (for example, a routed port, an SVI, a loopback port, or a tunnel port).

- The IPv6 function needs to be first enabled on a port.
- If a tracked host IP address is a link-local address, specify a network port.
- If a VRRP group (in the owner state) uses the actual IP address of an Ethernet port, the group priority is 255, and the monitored IP address or port can be configured, but the priority of the VRRP group is not changed.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the IPv6 function on the port.

ipv6 enable

(5) Configure a port to be monitored by an IPv6 VRRP group.

vrrp ipv6 *group-id* **track** { *interface-type interface-number* | **bfd** *interface-type interface-number peer-ipv6-address* } [*priority*]

No port to be monitored by an IPv6 VRRP group is configured by default. If a port to be monitored by an IPv6 VRRP group is configured and the priority parameter is not specified, the priority change value is 10.

(6) Configure an IPv6 address to be monitored by the IPv6 VRRP backup group.

vrrp ipv6 *group-id* **track** { *ipv6-global-address* | *ipv6-linklocal-address interface-type interface-number* } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

No IP address to be monitored by an IPv6 VRRP group is configured by default. If an IP address to be monitored by an IPv6 VRRP group is configured, the time interval for sending detection packets is 3 seconds, the timeout time for waiting for a response to a sent detection packet is 1 second, and the consecutive timeout count for judging that a tracked IP address is unreachable is 3.

(7) Configure the BFD support for IPv6 VRRP on an Interface.

vrrp ipv6 *group-id* **bfd** *ipv6-address*

By default, the linkage between an IPv6 VRRP and BFD is not configured on an interface. To enable such linkage, please configure this item.

(8) Exit back to the global configuration mode.

exit

(9) Configure the global IPv6 VRRP BFD.

vrrp ipv6 bfd *interface-type interface-number ipv6-address*

By default, global IPv6 VRRP BFD is not used to detect whether a master router is active. To enable this, please configure this item.

1.8 Configuring VRRP Attributes

1.8.1 Overview

If a VRRP backup group has been set up, you can configure enhancement to increase the usability of the VRRP backup group.

1.8.2 Configuration Tasks

The VRRP attribute configuration includes the following tasks:

All the following configuration tasks are optional and may be selected as needed.

- Configuring VRRP Basic Attributes
- Configuring a Method of Sending IPv4 VRRP Packets on a Super VLAN Port
- Configuring the Dual-Active Mode for an IPV4 VRRP Group
- Configuring the IPv4 VRRP Packet Version

1.8.3 Configuring VRRP Basic Attributes

1. Overview

If a VRRP backup group has been set up, you can configure basic attributes according to the actual situation.

2. Prerequisites

A VRRP backup group has been set up.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure VRRP basic attributes according to the actual situation.

- Configure a priority for the IPv4 VRRP backup group.

  vrrp *group-id* **priority** *priority*

  The default priority of an IPv4 VRRP backup group is **100**.

- Configure an authentication string of IPv4 VRRP.

  vrrp *group-id* **authentication** *authentication-string*

  No authentication string of IPv4 VRRP is configured by default.

- Configure a VRRP advertisement interval for the IPv4 VRRP master router.

  vrrp *group-id* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

  The default VRRP advertisement interval of the VRRP master router is **1** second.

- Configure the preemption mode for the IPv4 VRRP backup group.

  vrrp *group-id* **preempt** [**delay** *delay-seconds*]

  IPv4 VRRP runs in the preemption mode without preemption delay by default.

- Enable the IPv4 VRRP timer learning function.

  vrrp *group-id* **timers learn**

  The advertisement interval timer learning function is disabled for an IPv4 VRRP backup group by default.

- Configure a name for the IPv4 VRRP group.

  vrrp *group-id* **description** *group-name*

  No VRRP group name is configured by default.

- Configure a startup delay for the VRRP backup group on a port.

  vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }

  No VRRP group startup delay is configured by default.

1.8.4 Configuring a Method of Sending IPv4 VRRP Packets on a Super VLAN Port

1. Overview

The IPv4 VRRP protocol packets can be sent by the following three methods in a super VLAN. You can configure the method of sending advertisement packets.

- Sending IPv4 VRRP packets only to the first up sub VLAN in a super VLAN.
- Sending IPv4 VRRP packets to a specified sub VLAN in a super VLAN.
- Sending IPv4 VRRP packets to all the sub VLANs in a super VLAN.

2. Restrictions and Guidelines

- The configuration is effective only on super VLAN ports.
- If VRRP and VRRP plus are both enabled on a super VLAN port, VRRP packets are sent to all the up sub VLAN ports of the super VLAN port.

3. Prerequisites

VRRP has been enabled on a super VLAN port.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VLAN interface mode.

interface vlan *vlan-id*

(4) Configure the super VLAN mode.

supervlan

The super VLAN mode is not configured by default.

(5) Configure a sub VLAN range.

subvlan *vlan-range*

No sub VLAN range is configured by default.

(6) Configure a method of sending IPv4 VRRP packets on a super VLAN port.

vrrp detection-vlan { **first-subvlan** | *subvlan-id* }

The IPv4 VRRP packets on a super VLAN port are sent to the first up sub VLAN only by default.

1.8.5 Configuring the Dual-Active Mode for an IPV4 VRRP Group

1. Overview

A VRRP group works in master/backup mode by default. To set both ends of a VRRP group in the master state and avoid sending keepalive packets, configure the dual-active mode for the VRRP group.

2. Restrictions and Guidelines

- The dual-active mode can be configured only on a VLAN port.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VLAN interface mode.

interface vlan *vlan-id*

(4) Configure a VRRP group to work in dual-active state and configure the VRRP group not to send keepalive packets.

vrrp mode dual-active

A VRRP group works in master/backup mode by default.

1.8.6 Configuring the IPv4 VRRP Packet Version

1. Overview

The devices belonging to the same VRRP group should send packets according to the unified packet protocol: VRRPv2 or VRRPv3. By default, VRRPv2 is used for sending packets. VRRPv3 routers can recognize VRRPv2 packets, but VRRPv2 routers cannot recognize VRRPv3 packets. Configuring this function enables VRRPv3 routers to send VRRPv2 packets so as to communicate with VRRPv2 routers.

2. Restrictions and Guidelines

- The configuration is applicable to IPv4 VRRP only.
- If simple authentication has been configured for a VRRP group and the VRRP group is configured to send VRRPv2 packets, the authentication information is carried. If a VRRP group is configured to send VRRPv3 packets, the authentication information is not carried.
- The configuration only applies to the sending mode of VRRP packets and does not affect the receiving mode. For example, a VRRPv3 router can identify both VRRPv2 and VRRPv3 packets.

3. Prerequisites

IPv4 VRRP has been configured.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the VRRP packet standard for an IPv4 VRRP backup group.

vrrp *group-id* **version** { **2** | **3** }

IPv4 VRRP adopts the VRRPv2 standard by default.

1.9 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

You can run the **debug** command to output debugging information.

Caution

- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2 VRRP Monitoring

Command	Purpose
show [**ipv6**] **vrrp** [**brief** | *group-id*]	Displays the brief or detailed information of IPv4/IPv6 VRRP.
show [**ipv6**] **vrrp interface** *interface-type interface-number* [**brief**]	Displays the information of an IPv4/IPv6 VRRP group on a specified port.
show vrrp packet statistics [*interface-type interface-number*]	Displays the statistics of VRRP packets.
debug [**ipv6**] **vrrp**	Debugs VRRP errors, events, packets, and state.
debug [**ipv6**] **vrrp errors**	Debugs VRRP errors.
debug [**ipv6**] **vrrp events**	Debugs VRRP events.
debug vrrp packets [**acl** *acl-id* **|** [**icmp** | **protocol**] **interface** *interface-type interface-number* [*group-id*]] **debug ipv6 vrrp packets** [**acl** *acl-name* | [**icmp** | **protocol**] **interface** *interface-type interface-number* [*group-id*]]	Debugs VRRP packets.
debug [**ipv6**] **vrrp state**	Debugs VRRP state.

1.10 Configuration Examples

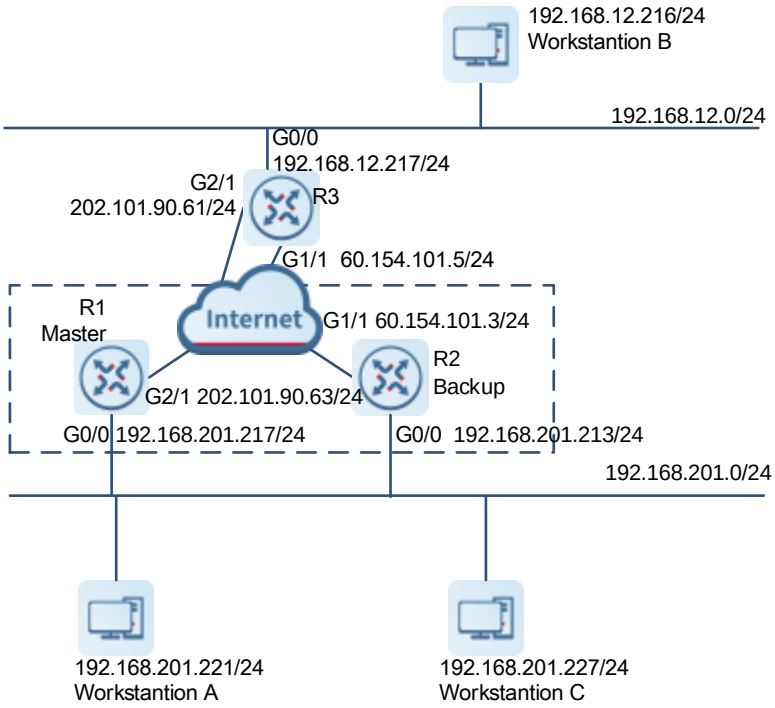
1.10.1 Configuring IPv4 VRRP

1. Requirements

An IPv4 VRRP group and a to-be-monitored port need to be configured.

2. Topology

Figure 1-9 Topology for Configuring a VRRP Group and a To-Be-Monitored Port



3. Notes

- Configure the work station cluster (192.168.201.0/24) to use the backup group composed of routers R1 and R2 and set the gateway address to the virtual router IP address configured for the backup group (192.168.201.1) so that the work station cluster accesses the remote work station cluster (192.168.12.0 /24) through the virtual router 192.168.201.1.
- On router R1, configure GigabitEthernet 2/1 as a VRRP monitored port.
- No VRRP but an ordinary routing function is configured on router 3.

4. Procedure

Perform the following configuration on router 3:

```
R3> enable
R3# configure terminal
R3(config)# interface GigabitEthernet 0/0
R3(config-if-GigabitEthernet 0/0)# no switchport
R3(config-if-GigabitEthernet 0/0)# ip address 192.168.12.217 255.255.255.0
```

```
R3(config-if-GigabitEthernet 0/0)# exit
R3(config)# interface GigabitEthernet 1/1
R3(config-if-GigabitEthernet 1/1)# no switchport
R3(config-if-GigabitEthernet 1/1)# ip address 60.154.101.5 255.255.255.0
R3(config-if-GigabitEthernet 1/1)# exit
R3(config)# interface GigabitEthernet 2/1
R3(config-if-GigabitEthernet 2/1)# no switchport
R3(config-if-GigabitEthernet 2/1)# ip address 202.101.90.61 255.255.255.0
R3(config-if-GigabitEthernet 2/1)# exit
R3(config)# router ospf
R3(config-router)# network 202.101.90.0 0.0.0.255 area 10
R3(config-router)# network 192.168.12.0 0.0.0.255 area 10
R3(config-router)# network 60.154.101.0 0.0.0.255 area 10
```

Perform the following configuration on router 1:

```
R1> enable
R1# configure terminal
R1(config)# interface GigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)# ip address 192.168.201.217 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# vrrp 1 priority 120
R1(config-if-GigabitEthernet 0/0)# vrrp 1 timers advertise 3
R1(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.201.1
R1(config-if-GigabitEthernet 0/0)# vrrp 1 track GigabitEthernet 2/1 30
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)# interface GigabitEthernet 2/1
R1(config-if-GigabitEthernet 2/1)# ip address 202.101.90.63 255.255.255.0
R1(config-if-GigabitEthernet 2/1)# exit
R1(config)# router ospf
R1(config-router)# network 202.101.90.0 0.0.0.255 area 10
R1(config-router)# network 192.168.201.0 0.0.0.255 area 10
```

Perform the following configuration on router 2:

```
R2> enable
R2# configure terminal
R2(config)# interface GigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)# ip address 192.168.201.213 255.255.255.0
R2(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.201.1
R2(config-if-GigabitEthernet 0/0)# vrrp 1 timers advertise 3
R2(config-if-GigabitEthernet 0/0)# exit
R2(config)# interface GigabitEthernet 1/1
R2(config-if-GigabitEthernet 1/1)# no switchport
R2(config-if-GigabitEthernet 1/1)# ip address 60.154.101.3 255.255.255.0
R2(config-if-GigabitEthernet 1/1)# exit
R2(config)# router ospf
R2(config-router)# network 60.154.101.0 0.0.0.255 area 10
R2(config-router)# network 192.168.201.0 0.0.0.255 area 10
```

5. Verification

Run the **show vrrp** command to verify the configuration.

Check whether router 1, which acts as the master router, reduces its VRRP backup group priority from 120 to 90 when GigabitEthernet2/1 connected to the wide area network (WAN) is unavailable. If yes, router 2 becomes the master router.

Check whether router 1 resumes its VRRP backup group priority from 30 to 120 when GigabitEthernet 2/1 connected to the WAN recovers. If yes, router 1 is reelected as the master router.

```
R1# show vrrp
GigabitEthernet 0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is 192.168.201.217 (local), priority is 120
  Master Down interval is 10.59 sec
  Tracking state of 1 interface, 1 up:
up   GigabitEthernet 2/1 priority decrement=30
```

Check the configuration on router 2.

```
R2# show vrrp
GigabitEthernet 0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is 192.168.201.217 , priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

6. Configuration Files

- Device R1 configuration file

```
hostname R1
!
interface GigabitEthernet 0/0
 no switchport
 ip address 192.168.201.217 255.255.255.0
 vrrp 1 priority 120
 vrrp 1 timers advertise 3
 vrrp 1 ip 192.168.201.1
```

```
 vrrp 1 track GigabitEthernet 2/1 30
!
interface GigabitEthernet 2/1
 no switchport
 ip address 202.101.90.63 255.255.255.0
!
router ospf
 network 202.101.90.0 0.0.0.255 area 10
 network 192.168.201.0 0.0.0.255 area 10
!
end
```

- Device R2 configuration file

```
hostname R2
!
interface GigabitEthernet 0/0
 no switchport
 ip address 192.168.201.213 255.255.255.0
 vrrp 1 timers advertise 3
 vrrp 1 ip 192.168.201.1
!
interface GigabitEthernet 1/1
 no switchport
 ip address 60.154.101.3 255.255.255.0
!
router ospf
 network 60.154.101.0 0.0.0.255 area 10
 network 192.168.201.0 0.0.0.255 area 10
!
end
```

- Device R3 configuration file

```
hostname R3
!
interface GigabitEthernet 0/0
 no switchport
 ip address 192.168.12.217 255.255.255.0
!
interface GigabitEthernet 1/1
 no switchport
 ip address 60.154.101.5 255.255.255.0
!
interface GigabitEthernet 2/1
 no switchport
 ip address 202.101.90.61 255.255.255.0
!
router ospf
```

```
 network 202.101.90.0 0.0.0.255 area 10
 network 192.168.12.0 0.0.0.255 area 10
 network 60.154.101.0 0.0.0.255 area 10
!

end
```

7. Common Errors

- Different virtual IP addresses of VRRP are configured on the routers in the same VRRP group, resulting in multiple master routers in the group.
- Different VRRP advertisement transmission intervals are configured on the routers in the same VRRP group and the timer learning function is not configured. As a result, multiple master routers arise in the group.
- Different VRRP packet versions are configured on the routers in the same VRRP group, resulting in multiple master routers in the group.
- For VRRPv2, the Ethernet ports of the routers in the same VRRP group all use the plaintext password authentication mode but use different authentication strings. As a result, multiple master routers arise in the group.

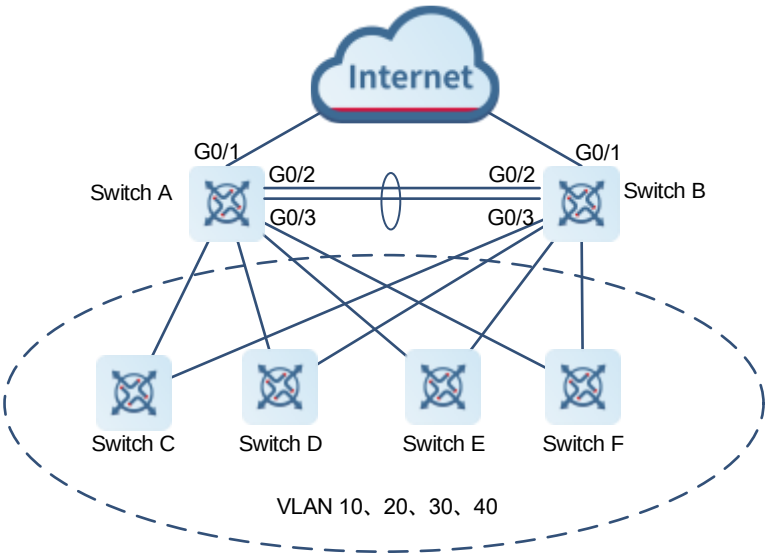
1.10.2 Configuring VRRP + MSTP

1. Requirements

As shown in Figure 1-10, VRRP and Multiple Spanning Tree Protocol (MSTP) can be configured to build a dual link backup network by using access devices and aggregation devices.

2. Topology

Figure 1-10 Topology for Configuring VRRP + MSTP



3. Notes

- Enable MSTP on devices (switches A, B, C, D, E, and F in this example). Configure VLAN-instance mappings (map VLANs 10 and 20 to instance 1, VLANs 30 and 40 to instance 2, and the rest VLANs to

instance 0), and configure gateway devices (switches A and B in this example) as the root bridges of corresponding instances.

- Add the SVIs of all VLANs to corresponding VRRP backup groups, and set gateways to the master and backup routers of corresponding backup groups. Table 1-3 lists the configuration details in the example.

Table 1-3 Parameters for VRRP + MSTP Topology Configuration

Gateway	VLAN ID	SVI	Backup Group	Virtual IP Address	State
Switch A	10	192.168.10.2	VRRP 10	192.168.10.1	Master
Switch B		192.168.10.3			Backup
Switch A	20	192.168.20.2	VRRP 20	192.168.20.1	Master
Switch B		192.168.20.3			Backup
Switch A	30	192.168.30.2	VRRP 30	192.168.30.1	Backup
Switch B		192.168.30.3			Master
Switch A	40	192.168.40.2	VRRP 40	192.168.40.1	Backup
Switch B		192.168.40.3			Master

- Configure the uplink ports (port GigabitEthernet 0/1 of switches A and B in the example) of master routers in backup groups as the monitored ports of the master routers.
  - Create VLANs. Create VLANs 10, 20, 30, and 40 on switches A and B.
  - Configure MST regions. Map VLANs 10 and 20 to instance 1, VLANs 20 and 30 to instance 2, and the rest VLANs to instance 0 on switches A and B.
  - Configure switch A as the root bridge of MST 0 and MST 1, and switch B as the root bridge of MST 2.
  - Enable MSTP.
  - Configure SVIs for all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the backup groups. Table 1-3 provides the corresponding configuration parameters.
  - Configure master routers and backup routers for all the groups.
  - Configure the uplink ports of master routers in VRRP backup groups as monitored ports (which must be L3 ports) of the VRRP groups.
  - Configure the interconnected ports of the core routers as an aggregate port (AP).

4. Procedure

(1) Perform the following configuration on Switch A:

Create VLANs 10, 20, 30, and 40.

```
SwitchA> enable
SwitchA# configure terminal
SwitchA(config)# vlan range 10,20,30,40
SwitchA(config)# exit
```

Map VLANs 10 and 20 to instance 1, VLANs 30 and 40 to instance 2, and the rest VLANs to instance 0.

```
SwitchA(config)# spanning-tree mst configuration
SwitchA(config-mst)# instance 1 vlan 10,20
SwitchA(config-mst)# instance 2 vlan 30,40
SwitchA(config-mst)# exit
```

On switch A, set the priority of MST 0 and MST 1 to **4096**, and the priority of MST 2 to **8192**.

```
SwitchA(config)# spanning-tree mst 0 priority 4096
SwitchA(config)# spanning-tree mst 1 priority 4096
SwitchA(config)# spanning-tree mst 2 priority 8192
```

Enable MSTP.

```
SwitchA(config)# spanning-tree
```

Configure SVIs for all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the backup groups.

```
SwitchA(config)# interface vlan 10
SwitchA(config-if-VLAN 10)# ip address 192.168.10.2 255.255.255.0
SwitchA(config-if-VLAN 10)# vrrp 10 ip 192.168.10.1
SwitchA(config-if-VLAN 10)# exit
SwitchA(config)# interface vlan 20
SwitchA(config-if-VLAN 20)# ip address 192.168.20.2 255.255.255.0
SwitchA(config-if-VLAN 20)# vrrp 20 ip 192.168.20.1
SwitchA(config-if-VLAN 20)# exit
SwitchA(config)# interface vlan 30
SwitchA(config-if-VLAN 30)# ip address 192.168.30.2 255.255.255.0
SwitchA(config-if-VLAN 30)# vrrp 30 ip 192.168.30.1
SwitchA(config-if-VLAN 30)# exit
SwitchA(config)# interface vlan 40
SwitchA(config-if-VLAN 40)# ip address 192.168.40.2 255.255.255.0
SwitchA(config-if-VLAN 40)# vrrp 40 ip 192.168.40.1
SwitchA(config-if-VLAN 40)# exit
```

Increase the priority of backup groups 10 and 20 on switch A to **120**.

```
SwitchA(config)# interface vlan 10
SwitchA(config-if-VLAN 10)# vrrp 10 priority 120
SwitchA(config-if-VLAN 10)# exit
SwitchA(config)# interface vlan 20
SwitchA(config-if-VLAN 20)# vrrp 20 priority 120
SwitchA(config-if-VLAN 20)# exit
```

Configure the port GigabitEthernet 0/1 of switch A as a route port, and set the IP address to10.10.1.1/24.

```
SwitchA(config)# interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)# no switchport
SwitchA(config-if-GigabitEthernet 0/1)# ip address 10.10.1.1 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)# exit
```

Configure the port GigabitEthernet 0/1 of switch A as the monitored port of backup groups 10 and 20, and set *Priority decrement* to 30.

```
SwitchA(config)# interface vlan 10
SwitchA(config-if-VLAN 10)# vrrp 10 track gigabitEthernet 0/1 30
SwitchA(config-if-VLAN 10)# exit
SwitchA(config)# interface vlan 20
SwitchA(config-if-VLAN 20)# vrrp 20 track gigabitEthernet 0/1 30
SwitchA(config-if-VLAN 20)# exit
```

Configure the ports GigabitEthernet 0/2 and GigabitEthernet 0/3 to belong to an AP, and configure the AP as a trunk port.

```
SwitchA(config)# interface range gigabitEthernet 0/2-3
SwitchA(config-if-range)# port-group 1
SwitchA(config)# interface aggregateport 1
SwitchA(config-if-AggregatePort 1)# switchport mode trunk
```

(2) Perform the following configuration on switch B:

Create VLANs 10, 20, 30, and 40.

```
SwitchB> enable
SwitchB# configure terminal
SwitchB(config)# vlan range 10,20,30,40
SwitchB(config-vlan-range)# exit
```

Map VLANs 10 and 20 to instance 1, VLANs 30 and 40 to instance 2, and the rest VLANs to instance 0.

```
SwitchB(config)# spanning-tree mst configuration
SwitchB(config-mst)# instance 1 vlan 10,20
SwitchB(config-mst)# instance 2 vlan 30,40
SwitchB(config-mst)# exit
```

On switch B, set the priority of MST 2 to **4096**, and the priority of MST 0 and MST 1 to **8192**.

```
SwitchB(config)# spanning-tree mst 2 priority 4096
SwitchB(config)# spanning-tree mst 0 priority 8192
SwitchB(config)# spanning-tree mst 1 priority 8192
```

Enable MSTP.

```
SwitchB(config)# spanning-tree
```

Configure SVIs for all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the backup groups.

```
SwitchB(config)# interface vlan 10
SwitchB(config-if-VLAN 10)# ip address 192.168.10.3 255.255.255.0
SwitchB(config-if-VLAN 10)# vrrp 10 ip 192.168.10.1
SwitchB(config-if-VLAN 10)# exit
SwitchB(config)# interface vlan 20
SwitchB(config-if-VLAN 20)# ip address 192.168.20.3 255.255.255.0
SwitchB(config-if-VLAN 20)# vrrp 20 ip 192.168.20.1
SwitchB(config-if-VLAN 20)# exit
SwitchB(config)# interface vlan 30
SwitchB(config-if-VLAN 30)# ip address 192.168.30.3 255.255.255.0
SwitchB(config-if-VLAN 30)# vrrp 30 ip 192.168.30.1
SwitchB(config-if-VLAN 30)# exit
```

```
SwitchB(config)# interface vlan 40
SwitchB(config-if-VLAN 40)# ip address 192.168.40.3 255.255.255.0
SwitchB(config-if-VLAN 40)# vrrp 40 ip 192.168.40.1
SwitchB(config-if-VLAN 40)# exit
```

Increase the priority of VRRP 30 and VRRP 40 on switch B to **120**.

```
SwitchB(config)# interface vlan 30
SwitchB(config-if-VLAN 30)# vrrp 30 priority 120
SwitchB(config-if-VLAN 30)# exit
SwitchB(config)# interface vlan 40
SwitchB(config-if-VLAN 40)# vrrp 40 priority 120
SwitchB(config-if-VLAN 40)# exit
```

Configure the port GigabitEthernet 0/1 of switch B as a route port, and set the IP address to 10.10.2.1/24.

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)# no switchport
SwitchB(config-if-GigabitEthernet 0/1)# ip address 10.10.2.1 255.255.255.0
SwitchB(config-if-GigabitEthernet 0/1)# exit
```

Configure the port GigabitEthernet 0/1 of switch B as the monitored port of backup groups 30 and 40, and set *Priority decrement* to 30.

```
SwitchB(config)# interface vlan 30
SwitchB(config-if-VLAN 30)# vrrp 30 track gigabitEthernet 0/1 30
SwitchB(config-if-VLAN 30)# exit
SwitchB(config)# interface vlan 40
SwitchB(config-if-VLAN 40)# vrrp 40 track gigabitEthernet 0/1 30
SwitchB(config-if-VLAN 40)# exit
```

Configure the ports GigabitEthernet 0/2 and GigabitEthernet 0/3 to belong to an AP, and configure the AP as a trunk port.

```
SwitchB (config)# interface range gigabitEthernet 0/2-3
SwitchB (config-if-range)# port-group 1
SwitchB (config)# interface aggregateport 1
SwitchB (config-if-AggregatePort 1)# switchport mode trunk
```

5. Verification

Run the **show run** and **show vrrp brief** commands to check whether the configuration is correct.

```
SwitchA# show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
```

```
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 4096
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1
!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.2 255.255.255.0
 vrrp 10 priority 120
 vrrp 10 ip 192.168.10.1
 vrrp 10 track GigabitEthernet 0/1 30
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.2 255.255.255.0
 vrrp 20 priority 120
 vrrp 20 ip 192.168.20.1
 vrrp 20 track GigabitEthernet 0/1 30
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.2 255.255.255.0
 vrrp 30 ip 192.168.30.1
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.2 255.255.255.0
 vrrp 40 ip 192.168.40.1
```

Check the VRRP state of device A.

```
SwitchA# show vrrp brief
```

```
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   120  3      -    P    Master  192.168.10.2  192.168.10.1
VLAN 20    20   120  3      -    P    Master  192.168.20.2  192.168.20.1
VLAN 30    30   100  3      -    P    Backup  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -    P    Backup  192.168.40.3  192.168.40.1
```

Disconnect the uplink of switch A and check the VRRP state of the device.

```
SwitchA# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   90   3      -    P    Backup  192.168.10.3  192.168.10.1
VLAN 20    20   90   3      -    P    Backup  192.168.20.3  192.168.20.1
VLAN 30    30   100  3      -    P    Backup  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -    P    Backup  192.168.40.3  192.168.40.1
```

Check the configuration of switch B.

```
SwitchB# show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
```

```
 no ip proxy-arp
 ip address 192.168.10.3 255.255.255.0
 vrrp 10 ip 192.168.10.1
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.3 255.255.255.0
 vrrp 20 ip 192.168.20.1
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.3 255.255.255.0
 vrrp 30 priority 120
 vrrp 30 ip 192.168.30.1
 vrrp 30 track GigabitEthernet 0/1 30
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.3 255.255.255.0
 vrrp 40 priority 120
 vrrp 40 ip 192.168.40.1
 vrrp 40 track GigabitEthernet 0/1 30
```

Check the VRRP state of device B.

```
SwitchB# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Backup  192.168.10.2  192.168.10.1
VLAN 20    20   100  3      -    P    Backup  192.168.20.2  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
```

Disconnect the uplink of switch B and check the VRRP state of the device.

```
SwitchB# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Master  192.168.10.3  192.168.10.1
VLAN 20    20   100  3      -    P    Master  192.168.20.3  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
```

6. Configuration Files

- Switch A configuration file

```
hostname SwitchA
!
vlan 10
!
vlan 20
!
```

```
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 4096
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1
!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.2 255.255.255.0
 vrrp 10 priority 120
 vrrp 10 ip 192.168.10.1
 vrrp 10 track GigabitEthernet 0/1 30
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.2 255.255.255.0
 vrrp 20 priority 120
 vrrp 20 ip 192.168.20.1
 vrrp 20 track GigabitEthernet 0/1 30
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.2 255.255.255.0
 vrrp 30 ip 192.168.30.1
!
interface VLAN 40
```

```
 no ip proxy-arp
 ip address 192.168.40.2 255.255.255.0
 vrrp 40 ip 192.168.40.1
```

- Switch B configuration file

```
hostname SwitchB
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.3 255.255.255.0
 vrrp 10 ip 192.168.10.1
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.3 255.255.255.0
 vrrp 20 ip 192.168.20.1
!
interface VLAN 30
```

```
 no ip proxy-arp
 ip address 192.168.30.3 255.255.255.0
 vrrp 30 priority 120
 vrrp 30 ip 192.168.30.1
 vrrp 30 track GigabitEthernet 0/1 30
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.3 255.255.255.0
 vrrp 40 priority 120
 vrrp 40 ip 192.168.40.1
 vrrp 40 track GigabitEthernet 0/1 30
```

7. Common Errors

- Different VRRP authentication modes are configured on the Ethernet ports of routers in the same VRRP group, resulting in multiple master routers in the group.
- For VRRPv2, the Ethernet ports of the routers in the same VRRP group all use the plaintext password authentication mode but use different authentication strings. As a result, multiple master routers arise in the group.
- Different VRRP advertisement transmission intervals are configured on the routers in the same VRRP group and the timer learning function is not configured. As a result, multiple master routers arise in the group.
- Different virtual IP addresses of VRRP are configured on the routers in the same VRRP group, resulting in multiple master routers in the group.

Contents

1 Configuring VRRP Plus 1
1.1 Introduction 1
1.1.1 Basic Concepts 1
1.1.2 Packet Structure 4
1.2 Configuration Task Summary 5
1.3 Configuring VRRP Plus 5
1.3.1 Overview 5
1.3.2 Restrictions and Guidelines 6
1.3.3 Procedure 6
1.4 Monitoring 7
1.5 Configuration Examples 7
1.5.1 Configuring IPv4 VRRP Plus 7
1.5.2 Configuring IPv6 VRRP Plus 10

1 Configuring VRRP Plus

1.1 Introduction

Virtual Router Redundancy Protocol Plus (VRRP Plus) is an extension of VRRP. It uses VRRP to implement gateway backup and load balancing in an IEEE 802.3 local area network (LAN). A backup router with VRRP enabled cannot forward packets. To use VRRP to implement load balancing, you need to manually configure multiple VRRP groups and set the gateway addresses of hosts in the LAN to virtual IP addresses of different VRRP groups. This increases the workload of the network administrator. VRRP Plus is designed to address this issue. VRRP Plus automatically implements load balancing. It automatically distributes traffic of different hosts to members of a VRRP Plus group, and you do not need to configure multiple VRRP groups or set the gateway addresses of hosts in the LAN to virtual IP addresses of different VRRP groups. This reduces the workload of the network administrator. You can enable a load balancing policy within a VRRP group without configuring multiple VRRP groups or different default gateways for hosts.

1.1.1 Basic Concepts

1. BVG

The balancing virtual gateway (BVG) allocates virtual MAC addresses to members of a VRRP Plus group. It responds to the gateway Address Resolution Protocol/Neighbor Discovery (ARP/ND) requests in the LAN, and forwards packets of hosts in the LAN.

2. BVF

The balancing virtual forwarder (BVF) forwards packets of hosts in the LAN. If a virtual MAC address is allocated to a BVF, the BVF participates in packet forwarding; otherwise, the BVF does not participate in packet forwarding.

3. Correlation with VRRP

VRRP Plus relies on VRRP, and runs in the following way:

- A master device in VRRP corresponds to a BVG in VRRP Plus.
- A backup device in VRRP corresponds to a BVF in VRRP Plus. Gateway addresses of hosts in a LAN are set to the virtual IPv4/IPv6 address of VRRP.

4. MAC Address Allocation

A BVG allocates virtual MAC addresses to BVFs. For an IPv4 VRRP Plus group, the BVG directly uses the virtual MAC address of VRRP to ensure compatibility between IPv4 VRRP Plus and IPv4 VRRP. That is, the virtual MAC address used by the BVG is 00-00-5E-00-01-{VRID} (VRID is the VRRP group number). The virtual MAC address used by a BVF is 00-1A-A9-16-{MemberID}-{VRID} (MemberID is the member ID of the BVF in the VRRP Plus group). Currently, a VRRP Plus group can have up to four members. The BVG uses the member ID 01, and the other BVFs use the member IDs 02 to 04.

For an IPv6 VRRP Plus group, the BVG directly uses the virtual MAC address of IPv6 VRRP to ensure compatibility between IPv6 VRRP Plus and IPv6 VRRP. That is, the virtual MAC address used by the BVG is

00-00-5E-00-02-{VRID} (VRID is the IPv6 VRRP group number). The virtual MAC address used by a BVF is 14-14-4B-72-{76 + MemberID }-{VRID}. The value range of MemberID is from 01 to 03.

5. Load Balancing Policies

The BVG responds to the gateway ARP/NS requests sent from hosts in a LAN. According to a specific load balancing policy, the BVG responds to hosts by using different virtual MAC addresses. The following load balancing policies are available:

- Host-dependent policy: A specific virtual MAC address is used to respond to the requests sent by a specific host.
- Round-robin policy: Virtual MAC addresses in a backup group are used in a cyclic manner to respond to the gateway ARP/NS requests sent by hosts.
- Weighted policy: The ARP/NA requests are responded based on the forwarding capability of a device.

Policy switching is described below:

- If the load balancing mode is changed, load balancing is always implemented in the new load balancing mode. For example, if the round-robin load balancing mode is previously used, and later the weighted mode is used, load balancing is implemented in weighted mode. Load balancing cannot be implemented for hosts that have learned the VRRP virtual gateway addresses before the configuration of VRRP Plus. Therefore, if VRRP Plus is configured after a VRRP group switches to the master state, real load balancing cannot be implemented before aging of the ARP/ND entries learned by hosts. Load balancing is implemented only after the gateway ARP/ND entries learned by the hosts age and the hosts request new gateway addresses.
- Weight configuration means configuring different weights for different devices. In this way, more traffic is distributed to the device with a greater weight and less traffic is distributed to the device with a smaller weight, thereby fully utilizing the forwarding performance of different devices (if the total weight of virtual routers in a VRRP Plus group is 0, the ARP/NS requests are not responded). When the weight of a BVF in a backup group is smaller than the lower threshold, the BVF automatically exits the forwarding role. When the weight recovers and is greater than the upper threshold, the BVF automatically applies to the forwarding role. The forwarding role can be recovered when one or more remaining virtual MAC addresses or proxy virtual MAC addresses exist.
- The function of periodically sending of gratuitous ARP packets on an interface also affects the load balancing function of VRRP Plus. When VRRP Plus is enabled, the function of sending gratuitous ARP/NA packets of VRRP virtual IP addresses will be disabled. When a virtual IP address overlaps with an actual IP address, gratuitous ARP/NA packets of this address are no longer sent.
- When an address conflict occurs between a host and the local device, the ARP/NA module will broadcast gratuitous ARP/NA packets of this address. If a conflict occurs on the VRRP Plus virtual address, sending gratuitous ARP/NA packets results in re-learning of the host's gateway MAC address, which negatively affects the load balancing function of VRRP Plus. Therefore, the load balancing function of VRRP Plus is currently not supported in this scenario.

6. Proxy Virtual MAC Address

When a device with a virtual MAC address assigned becomes faulty in a backup group, traffic of hosts that use this virtual MAC address as the gateway MAC address will be interrupted. The BVG in the VRRP Plus backup group can quickly detect the fault, and automatically allocate the virtual MAC address of the faulty BVF to another device in the backup group. The new device acts as the proxy of the faulty device to forward packets of

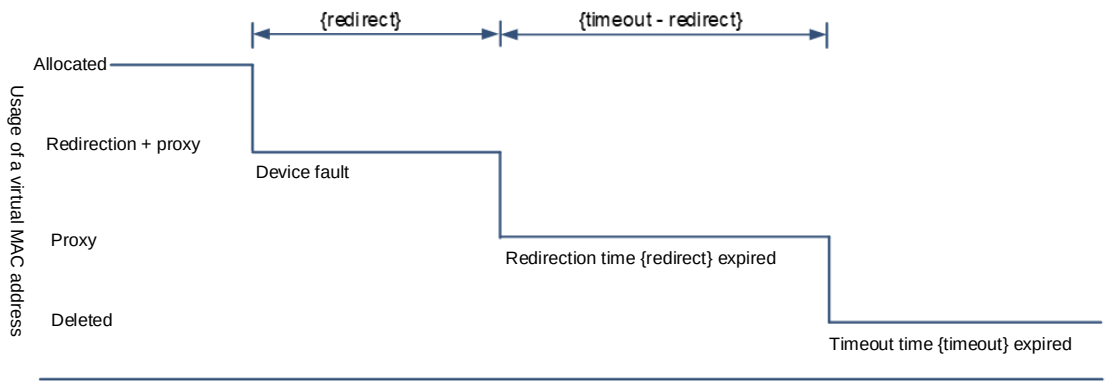
the virtual MAC address. In addition, this proxy device takes over traffic of original hosts to prevent traffic interruption. The virtual MAC address allocated to a device in a backup group can be called a master virtual MAC address, and the virtual MAC address used by this device on behalf of another device is called a proxy virtual MAC address.

7. Redirection Interval and Timeout

VRRP Plus provides the virtual MAC address proxy function so that another device can take the place of a faulty device with a virtual MAC address assigned to forward packets. If a BVF recovers from the fault, its forwarding role should be restored and the BVF continues to forward packets of the virtual MAC address allocated to this BVF. If the faulty BVF does not recover all the time, the backup group stops redirecting traffic to this virtual MAC address. That is, when gateway ARP requests are received again, this virtual MAC address is no longer used to give responses. After a sufficient long period of time, it is believed that hosts that use the virtual MAC address as the gateway MAC address already update the ARP/ND table entry of the gateway address, and the traffic is already taken over by other devices. Now, this virtual MAC address can be deleted, and packets sent to this virtual MAC address should be discarded.

VRRP Plus allows configuring the redirection interval and timeout for a backup group. When a device is faulty, the backup group allocates the virtual MAC address of the faulty device to another device. Within the redirection interval, the backup group continues to use this virtual MAC address to respond to the ARP/NS requests. When the redirection time expires, the backup group no longer uses this virtual MAC address to respond to the requests. When the timeout time elapses, the backup group deletes this virtual MAC address and stops using it for proxy forwarding. Figure 1-1 shows the changes in the role of a virtual MAC address within the redirection interval and timeout time.

Figure 1-1 Diagram of Changes in the Role of an Allocated Virtual MAC Address



8. Correlation with Track

VRRP Plus supports correlation with bidirectional forwarding detection (BFD) and can adjust the weight based on the link status. Each device in a backup group can associate its weight with the link status. When a link is abnormal or unreachable, the device automatically decreases its weight. When the weight is too low, the device automatically exits the forwarding role. If a backup group is currently using the weighted load balancing policy, traffic can be distributed based on the new weight. When the associated link recovers, the device automatically restores its original weight and the forwarding role. If the backup group is currently using the weighted load balancing policy, traffic is distributed based on the restored weight.

9. Forwarding Preemption

VRRP Plus supports the function of preempting the forwarding role. In VRRP Plus, at most four devices can participate in load balancing. That is, a VRRP Plus backup group generates at most four virtual MAC addresses. If more than four devices are added to a VRRP Plus group, only four devices participate in packet forwarding. The remaining devices only listen to the statuses of other devices and do not participate in packet forwarding. Only when a device participating in packet forwarding is faulty, another device that originally does not participate in packet forwarding takes the place of the faulty device to forward packets. Assume that a VRRP Plus backup group already has four devices and all these devices participate in packet forwarding; a fifth device is added to the VRRP Plus group, and the forwarding capability of this device is strong or a device taking the forwarding role encounters a link failure and consequently the degradation of forwarding performance. In this case, if the preemption mode is enabled, the fifth device preempts the forwarding role from a device with a smaller weight (that is, with weaker forwarding capability). A greater weight is configured for a device with stronger forwarding capability. When the weight of a device in listening state is greater than that of a forwarding device, the device in listening state automatically preempts the forwarding role from the forwarding device. That is, the device with stronger forwarding capability forwards packets, whereas the device with lower forwarding capability is in listening state. This minimizes the waste of resources.

The BVG in a backup group is responsible for allocating virtual MAC addresses. Therefore, the BVG role cannot be preempted, and only the forwarding role of a BVF can be seized. If the BVG is faulty, VRRP re-elects a new master device, which assumes the BVG role.

1.1.2 Packet Structure

Figure 1-2 shows the structure of VRRP Plus packets.

Figure 1-2 Structure of VRRP Plus Packets

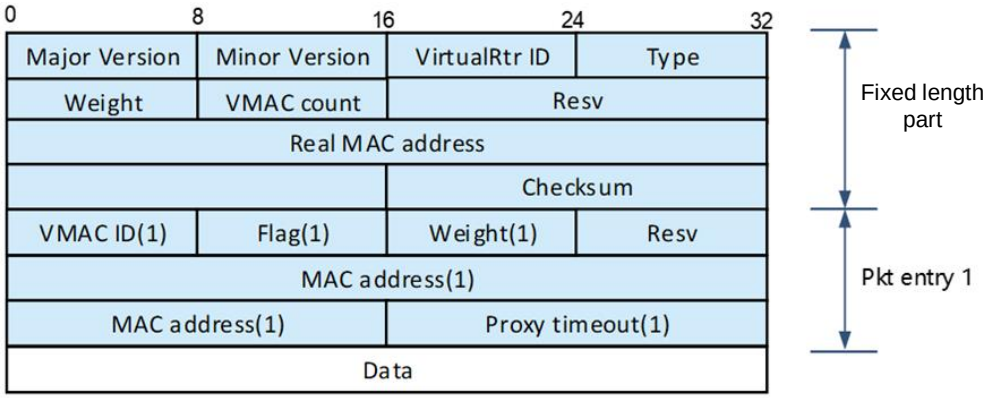


Table 1-1 Field Description of VRRP Plus Packets

Packet Field	Description
Major Version	Major version number. The current version is 1.
Minor Version	Minor version number. The current version is 0.
VirtualRtr ID	Virtual router ID, that is, the ID of a VRRP Plus backup group.

Packet Field	Description
Type	Type of VRRP Plus packets. Values and corresponding types are as follows: ● **0**: Indicates a tricky packet. ● **1**: Indicates a virtual MAC request packet. ● **2**: Indicates a keepalive packet of a BVF. ● **3**: Indicates the virtual MAC address release packet sent by the BVF to the BVG. ● **4**: Indicates the virtual MAC address allocation packet sent by the BVG to a BVF.
Weight	Weight of the device.
VMAC count	Number of virtual MAC addresses filled in the packet.
Resv	Reserved field in the fixed length part.
Real MAC address	Real MAC address of the interface on the local device.
Checksum	Packet checksum (including the fixed length part and filling part).
VMAC ID	Filled virtual MAC ID.
Flag	Flag information of the virtual MAC address.
Weight	Weight of the device to which the virtual MAC address is allocated.
Resv	Reserved field in the filling part.
MAC address	Real MAC address of the interface on the device to which the virtual MAC address is allocated.
Proxy timeout	Remaining time before timeout of the virtual MAC address filling in the case of a proxy virtual MAC address.

1.2 Configuration Task Summary

VRRP Plus configuration includes the following tasks:

(1) Configuring VRRP Plus

1.3 Configuring VRRP Plus

1.3.1 Overview

This section describes how to enable the VRRP Plus function and adjust the VRRP Plus weight based on the track object, to implement automatic balancing among multiple backup groups.

1.3.2 Restrictions and Guidelines

To enable the VRRP Plus function, you must configure a VRRP virtual IP address for the corresponding backup group.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L3 interface configuration mode.

interface *interface-type interface-number*

(4) Enable IPv4 VRRP.

vrrp *group-id* **ip** *ipv4-address* [**secondary**]

IPv4 VRRP is disabled on a port by default.

(5) Configure a priority for the IPv4 VRRP backup group.

vrrp *group-id* **priority** *Priority*

The default priority of an IPv4 VRRP backup group is **100**.

(6) Enable the VRRP Plus function on the interface.

vrrp [**ipv6**] *group-id* **balance**

The VRRP Plus function is disabled by default.

(7) Configure a VRRP Plus load balancing policy.

vrrp [**ipv6**] *group-id* **load-balancing** { **host-dependent** | **round-robin** | **weighted** }

By default, VRRP Plus uses the host-dependent load balancing policy, that is, host-dependent.

(8) Configure the redirection interval and timeout time for proxy virtual MAC addresses of the VRRP Plus backup group.

vrrp [**ipv6**] *group-id* **timers redirect** *redirect-interval redirect-timeout*

The default redirection interval of proxy virtual MAC addresses of a VRRP Plus backup group is **300** seconds and the default redirection timeout time is **14400** seconds.

(9) Configure the weight and upper and lower thresholds for the VRRP Plus backup group.

vrrp [**ipv6**] *group-id* **weighting** *weight-limit* [**lower** *min-weight-value*] [**upper** *max-weight-value*]

The default weight, default upper threshold, and default lower threshold of a VRRP Plus backup group are **100**, **1**, and **100** respectively.

(10) Configure the forwarding preemption function for the VRRP Plus backup group.

vrrp [**ipv6**] *group-id* **forwarder preempt**

The forwarding preemption function is enabled for a VRRP Plus backup group by default.

(11) Configure a track object for adjusting the weight for the VRRP Plus backup group.

vrrp [**ipv6**] *group-id* **weighting track** *object-number* [**decrement** *value*]

VRRP Plus tracking is not configured by default.

1.4 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2 VRRP Plus Monitoring

Command	Purpose
show [**ipv6**] **vrrp balance**	Displays the brief or detailed information about VRRP Plus.
show [**ipv6**] **vrrp balance interface** *interface-type interface-number* [**brief**]	Displays the actions of a VRRP Plus group on a specified interface.
debug [**ipv6**] **vrrp balance**	Debugs the VRRP Plus function.
debug [**ipv6**] **vrrp balance error**	Debugs errors.
debug [**ipv6**] **vrrp balance event**	Debugs events of a VRRP Plus group.
debug [**ipv6**] **vrrp balance messages**	Debugs messages of VRRP Plus.
debug [**ipv6**] **vrrp balance packets**	Debugs the VRRP Plus packets.
debug [**ipv6**] **vrrp balance state**	Debugs the VRRP Plus group status.
debug vrrp balance timer	Debugs the timers of a VRRP Plus group.
debug [**ipv6**] **vrrp balance**	Debugs the VRRP Plus function.
debug [**ipv6**] **vrrp balance error**	Debugs errors.

1.5 Configuration Examples

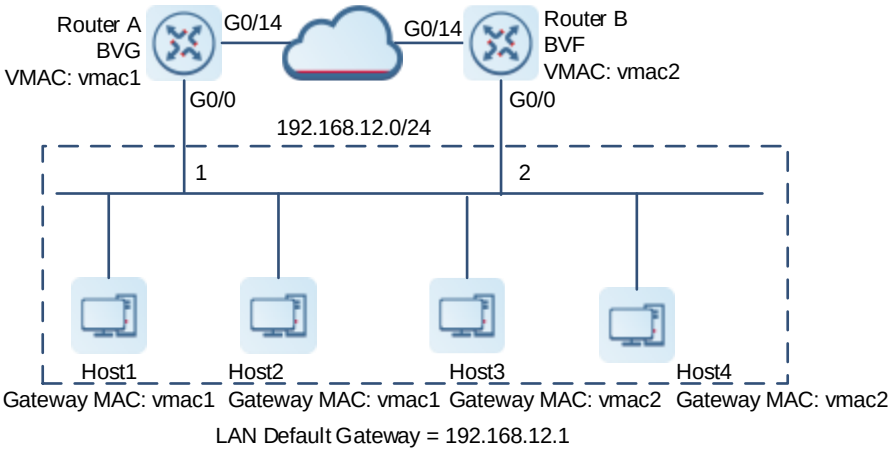
1.5.1 Configuring IPv4 VRRP Plus

1. Requirements

A load balancing policy needs to be enabled in an IPv4 VRRP group.

2. Topology

Figure 1-3 Topology for Configuring IPv4 VRRP Plus



3. Notes

- Configure a VRRP group and enable VRRP Plus on both routers A and B. Configure the local IP addresses so that router A becomes the BVG (master) device and router B becomes a BVF (backup) device.
- Configure the weighted load balancing policy for VRRP Plus. Configure a track object for adjusting the weight, and set the weight decrement value to 100.
- Retain default configurations for the weight, upper and lower thresholds, redirection interval, timeout time, and forwarding preemption function of the backup group.
- Set the default gateway addresses of hosts 1 to 4 in the LAN to the virtual IP address of VRRP, that is, 192.168.12.1.

4. Procedure

Perform the following configuration on router A:

```
RouterA> enable
RouterA# configure
RouterA(config)# interface GigabitEthernet0/0
RouterA(config-if-GigabitEthernet 0/0)# no switchport
RouterA(config-if-GigabitEthernet 0/0)# ip address 192.168.12.3 255.255.255.0
RouterA(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.12.1
RouterA(config-if-GigabitEthernet 0/0)# vrrp 1 balance
RouterA(config-if-GigabitEthernet 0/0)# vrrp 1 load-balancing weighted
```

Perform the following configuration on router B:

```
RouterB> enable
RouterB# configure
RouterB(config)# interface GigabitEthernet0/0
RouterB(config-if-GigabitEthernet 0/0)# no switchport
RouterB(config-if-GigabitEthernet 0/0)# ip address 192.168.12.2 255.255.255.0
RouterB(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.12.1
```

```
RouterB(config-if-GigabitEthernet 0/0)# vrrp 1 balance
RouterB(config-if-GigabitEthernet 0/0)# vrrp 1 load-balancing weighted
```

5. Verification

Run the **show vrrp balance** command to display the configuration of the VRRP Plus backup group. If the backup group has packet forwarding tasks, "local" is displayed in the "Forwarder" column, and the virtual MAC address allocated to this backup group is also displayed.

```
RouterA# show vrrp balance interface GigabitEthernet0/0
State is BVG
  Virtual IP address is 192.168.12.1
  Hello time 1 sec, hold time 3 sec
  Load balancing: weighted
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 100 (configured 100), thresholds: lower 1, upper 100
  There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0101
    Owner ID is 0000.0001.0006
    Preemption disabled (BVG cannot be preempted)
  Forwarder 2
    MAC address:
001a.a916.0201
    Owner ID is 00d0.f822.33a3
Preemption enabled
```

```
RouterB# show vrrp balance interface GigabitEthernet0/0
  State is BVF
  Virtual IP address is 192.168.12.1
  Hello time 1 sec, hold time 3 sec
  Load balancing: weighted
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 100 (configured 100), thresholds: lower 1, upper 100
  There are 2 forwarders
  Forwarder 1
    MAC address:
      0000.5e00.0101
    Owner ID is 0000.0001.0006
    Preemption disabled (BVG cannot be preempted)
  Forwarder 2 (local)
    MAC address:
001a.a916.0201
    Owner ID is 00d0.f822.33a3
    Preemption enabled
```

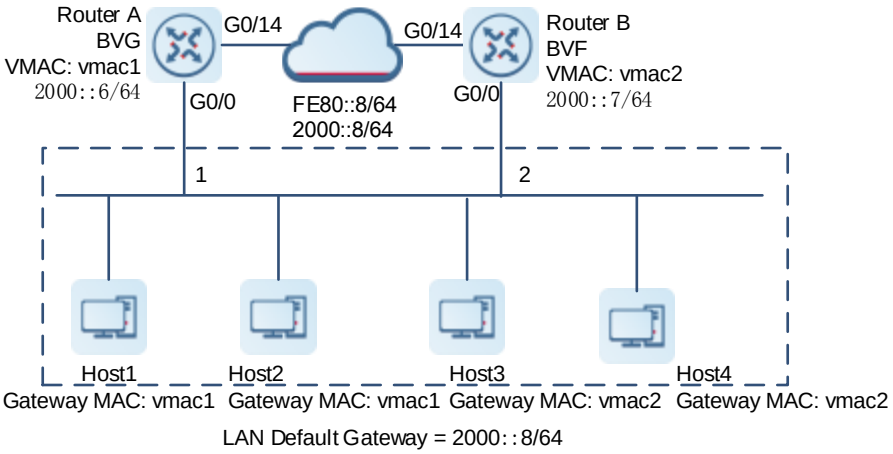
1.5.2 Configuring IPv6 VRRP Plus

1. Requirements

A load balancing policy needs to be enabled in an IPv6 VRRP group.

2. Topology

Figure 1-4 Topology for Configuring IPv6 VRRP Plus



3. Notes

- Configure an IPv6 VRRP group and enable IPv6 VRRP Plus on both routers A and B. Configure the priorities so that router A becomes the BVG (master) device and router B becomes a BVF (backup) device.
- Configure the weighted load balancing policy for the IPv6 VRRP Plus backup group.
- Retain default configurations for the weight, upper and lower thresholds, redirection interval, timeout time, and forwarding preemption function of the backup group.
- Hosts 1 to 4 are hosts in the LAN. Set their IPv6 gateway addresses to 2000::8.

4. Procedure

Perform the following configuration on router A:

```
RouterA> enable
RouterA# configure
RouterA(config)# interface GigabitEthernet0/0
RouterA(config-if-GigabitEthernet 0/0)# no switchport
RouterA(config-if-GigabitEthernet 0/0)# ipv6 address 2000::6/64
RouterA(config-if-GigabitEthernet 0/0)# vrrp 1 ipv6fe80::8
RouterA(config-if-GigabitEthernet 0/0)# vrrp 1 ipv62000::8
RouterA(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 priority 120
RouterA(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 load-balancing weighted
RouterA(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 balance
```

Perform the following configuration on router B:

```
RouterB> enable
```

```
RouterB# configure
RouterB(config)# interface GigabitEthernet0/0
RouterB(config-if-GigabitEthernet 0/0)# no switchport
RouterB(config-if-GigabitEthernet 0/0)# ipv6 address 2000::7/64
RouterB(config-if-GigabitEthernet 0/0)# vrrp 1 ipv6fe80::8
RouterB(config-if-GigabitEthernet 0/0)# vrrp 1 ipv62000::8
RouterB(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 load-balancing weighted
RouterB(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 balance
```

5. Verification

Run the **show ipv6 vrrp balance** command to display the configuration of the VRRP Plus backup group. If the backup group has packet forwarding tasks, "local" is displayed in the "Forwarder" column, and the virtual MAC address allocated to this backup group is also displayed.

```
RouterA# show ipv6 vrrp balance interface GigabitEthernet0/0
GigabitEthernet 0/0 - Group 1
  State is BVG
  Virtual IPv6 address is as follows:
    FE80::8
    2000::8
  Hello time 1 sec, hold time 3 sec
  Load balancing: weighted
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 100 (configured 100), thresholds: lower 1, upper 100
  There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0201
    Owner ID is 00d0.f8fb.96f3
    Preemption disabled (BVG cannot be preempted)
  Forwarder 2
    MAC address:
      1414.4b72.7701
    Owner ID is 00d0.f8fb.6c42
    Preemption enabled
```

```
RouterB# show ipv6 vrrp balance interface GigabitEthernet0/0
GigabitEthernet 0/0 - Group 1
  State is BVF
  Virtual IPv6 address is as follows:
    FE80::8
    2000::8
  Hello time 1 sec, hold time 3 sec
  Load balancing: weighted
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 150 (configured 150), thresholds: lower 1, upper 100
```

```
  There are 2 forwarders
  Forwarder 1
    MAC address:
      0000.5e00.0201
    Owner ID is 00d0.f8fb.96f3
    Preemption disabled (BVG cannot be preempted)
  Forwarder 2 (local)
    MAC address:
      1414.4b72.7701
    Owner ID is 00d0.f8fb.6c42
Preemption enabled
```

6. Common Errors

- VRRP Plus does not take effect because no VRRP virtual IP address is configured for a group.

Contents

1 Configuring BFD 1
1.1 Introduction 1
1.1.1 Basic Concepts 1
1.1.2 Session Establishment 3
1.1.3 Session Detection 5
1.1.4 BFD Support for Applications 6
1.1.5 BFD Protection 9
1.1.6 BFD Flapping Advertisement Dampening 9
1.1.7 SBFD Reflector Establishment 9
1.1.8 Protocols and Standards 10
1.2 Restrictions and Guidelines 10
1.3 Configuration Task Summary 11
1.4 Configuring BFD Basic Functions 11
1.4.1 Overview 11
1.4.2 Configuration Tasks 11
1.4.3 Configuring BFD Parameters 12
1.4.4 Configuring the BFD Echo Mode 12
1.4.5 Configuring the BFD Slow Timer 13
1.4.6 Configuring BFD Support for L3 Interfaces 13
1.4.7 Configuring BFD Support for Applications 14
1.5 Configuring BFD Protection 15
1.5.1 Overview 15
1.5.2 Restrictions and Guidelines 16

1.5.3 Prerequisites 16

1.5.4 Procedure 16

1.6 Configuring BFD Flapping Advertisement Dampening 16

1.6.1 Overview 16

1.6.2 Restrictions and Guidelines 16

1.6.3 Procedure 16

1.7 Configuring an SBFD Reflector 17

1.7.1 Overview 17

1.7.2 Restrictions and Guidelines 17

1.7.3 Procedure 17

1.8 Monitoring 17

1.9 Configuration Examples 18

1.9.1 Configuring BFD Support for OSPF 18

1 Configuring BFD

1.1 Introduction

Bidirectional forwarding detection (BFD) provides a light-load and fast method for detecting the connectivity of the forwarding path between two adjacent devices. It quickly detects faults on the bidirectional forwarding path between two devices for upper layer protocols such as routing protocols and Multi-Protocol Label Switching (MPLS) so that measures can be taken in a timely manner to guarantee services. BFD minimizes the impact of faults on services and improves network availability.

1.1.1 Basic Concepts

1. Packet Format

Detection packets transmitted by BFD are User Datagram Protocol (UDP) packets, which are classified into two types:

- Control packets: The protocol defines a specific format, as shown in Figure 1-1. Currently, there are two versions (v0 and v1) for the format of control packets: v1 is adopted by default for establishing a BFD session; if a device receives packets of v0 from the peer system, the device automatically switches to v0.
- Echo packets: Echo packets are only used by the local system of a BFD session, and the protocol does not define a specific format.

Figure 1-1 BFD Packet Format

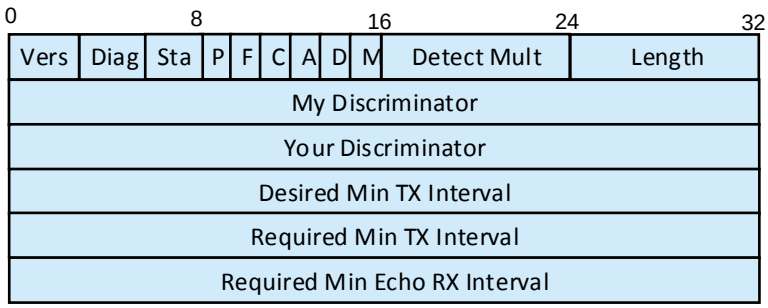


Table 1-1 Description of BFD Packet Fields

Field	Description
Vers	BFD protocol version number, which is 1 currently.

Field	Description
Diag	Causes for the local system to switch from up state to another state last time, including: **0**: Indicates no diagnostic information. **1**: Controls timeout detection. **2**: Indicates that the echo function failed. **3**: Indicates that a neighbor advertises session down. **4**: Indicates forwarding plane reset. **5**: Indicates that the path failed. **6**: Indicates that the connection path failed. **7**: Indicates that the local system enters the AdminDown state.
Sta	BFD local session states, including: **0**: Indicates the AdminDown state. **1**: Indicates the Down state. **2**: Indicates the Init state. **3**: Indicates the Up state.
P	The transmitter sets this flag to **1** in a BFD packet upon parameter changes. The receiver must immediately respond to this packet.
F	This flag must be set to **1** in the response packet for responding to the P flag that is set to **1**.
C	Forwarding/control separation flag. If it is set to **1**, the control plane changes do not affect BFD detection. For example, if the control plane is Open Shortest Path First (OSPF), when OSPF is restarted or experiences graceful restart (GR), BFD can continue to detect the link state.
A	Authentication flag. If it is set to **1**, a session needs to be authenticated.
D	Query request. If it is set to **1**, the transmitter desires the query mode for detecting links.
M	It is used in point-to-multipoint applications in the future. It must be set to **0** currently.
Detect Mult	Detection timeout multiplier. It is used by the detector to calculate the detection timeout time.
Length	Packet length.
My Discriminator	Discriminator of the local end of a BFD session.
Your Discriminator	Discriminator of the remote end of a BFD session
Desired Min Tx Interval	Minimum BFD packet transmission interval supported by the local end.

Field	Description
Required Min RX Interval	Minimum BFD packet receiving interval supported by the local end.
Required Min Echo RX Interval	Minimum echo packet receiving interval supported by the local end. It is set to **0** if the local end does not support the echo function.
Auth Type	Authentication type. It is an optional field and can be set to the following values: Simple Password Keyed MD5 Meticulous Keyed MD5 Keyed SHA1 Meticulous Keyed SHA1
Auth Length	Authentication data length.
Authentication Data	Authentication data area.

2. Session State

BFD migrates the state machine based on the local session state and the BFD packets received from the peer end. A BFD state machine is established and torn down using a three-way handshake mechanism, to ensure that both ends know the state change. A BFD session can be in any of the following four basic states:

- Down: Indicates that a session is in the down state or is established just now.
- Init: Indicates that the local system has communicated with the peer system and desires to bring the session to the up state.
- Up: Indicates that a session has been established successfully.
- AdminDown: Indicates that a session is in the AdminDown state.

3. Transmission Interval and Detection Time

During the establishment of a BFD session, both ends negotiate about BFD parameters to determine the transmission interval and detection time. After a BFD session is established, both ends dynamically negotiate about BFD parameters (for example, the minimum transmission interval and minimum receiving interval). After protocols at both ends transmit relevant negotiation packets, they adopt the new transmission interval and detection time, without affecting the current state of the session.

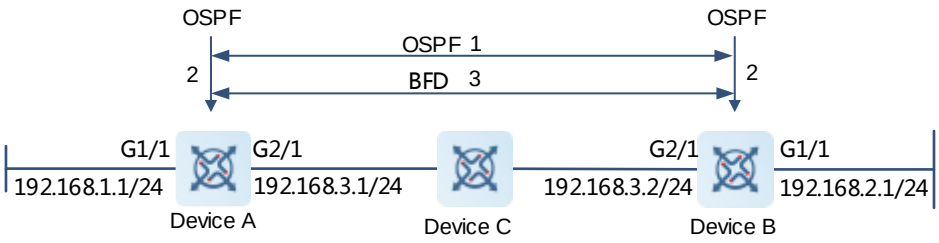
1.1.2 Session Establishment

BFD detection starts from the establishment of a BFD session.

1. Session Establishment Process

BFD itself is unable to discover neighbors. It needs an upper-layer protocol to specify the neighbor, with which BFD needs to establish a session. As shown in Figure 1-2, two devices running OSPF and BFD are connected through an L2 device.

Figure 1-2 BFD Session Establishment



The BFD session establishment process is as follows:

- OSPF discovers a neighbor and establishes a connection with the neighbor.
- OSPF instructs BFD to establish a session with the neighbor.
- BFD establishes a session with the neighbor.

2. Session Establishment Mode

The BFD protocol specifies that a BFD session can be established in two modes:

- Active mode: Before the establishment of a session, BFD actively transmits a control packet for establishing a BFD session regardless of whether it receives a control packet for establishing a BFD session from the peer end.
- Passive mode: BFD does not actively transmit a control packet for establishing a BFD session before a session is established but waits till it receives a control packet for establishing a BFD session from the peer end.

Specification

The passive mode is not supported currently.

3. Negotiation of Session Parameters

Both ends negotiate about BFD session parameters during the establishment of a BFD session, to determine the transmission interval and detection time. Pay attention to the following points:

- BFD session parameters (including the minimum transmission interval, minimum receiving interval, and detection timeout multiplier) must be set for interfaces at both ends. Otherwise, a BFD session cannot be established.
- Interfaces at both ends negotiate about BFD session parameters and detect the session based on the parameters during the establishment of a BFD session.
- After a BFD session is established, both ends dynamically negotiate about BFD parameters (for example, the minimum transmission interval and minimum receiving interval). After protocols at both ends transmit relevant negotiation packets, they adopt the new transmission interval and detection time, without affecting the current state of the session.
- BFD session parameters can be updated only after all the original sessions on a port complete negotiation; otherwise an error is prompted. You can run a related command to query the negotiation status of the original sessions.

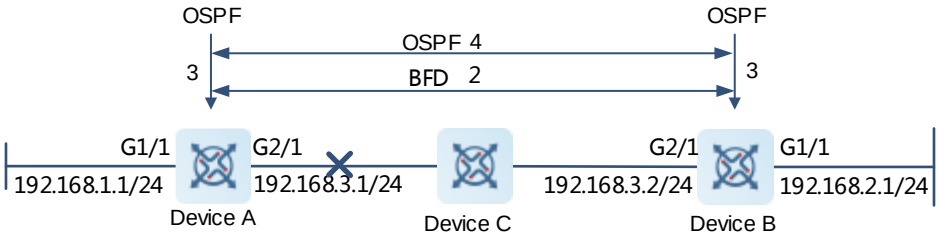
1.1.3 Session Detection

Link detection starts after the establishment of a BFD session. BFD periodically transmits BFD control packets. If it fails to receive BFD packets from the peer end within the detection time, it deems that the session is down and instructs the associated application to accelerate the convergence.

1. Detection Process

As shown in Figure 1-3, two devices running OSPF and BFD are connected through an L2 device.

Figure 1-3 Topology for BFD Session Detection



The handling process after a BFD session is down is as follows:

- The link between Device A and Device C fails.
- The BFD session between Device A and Device B detects the failure.
- BFD notifies the local OSPF that the forwarding path to the neighbor is faulty.
- OSPF processes the neighbor down situation. If a backup forwarding path is available, it starts protocol convergence to enable the backup forwarding path.

2. Detection Mode

BFD supports the following detection modes:

- Asynchronous mode

  In asynchronous mode, systems transmit BFD control packets periodically to each other. If a system fails to receive BFD control packets from the peer end within the detection time, it advertises that the session is down.

- Query mode

  In query mode, it is assumed that each system has an independent method for confirming its connection with other systems. After a BFD session is established, the system stops transmitting BFD control packets unless it needs to explicitly verify the connectivity. In such a case, the system transmits a shot-sequence BFD control packet. If the system fails to receive a returned packet within the detection time, it advertises that the session is down. If it receives a response from the peer end, the forwarding path is reachable.

- Echo mode

  In echo mode, the local system periodically transmits BFD echo packets and a remote system receives and loops back the packets through the forwarding path. If the local system fails to receive several consecutive echo packets within the detection time, it advertises that the session is down. The echo function can be used together with the preceding two detection modes. The echo packet detection function does not require the involvement of the control plane of the remote system. Packets are returned by the forwarding

plane of the remote system, which reduces the delay and ensures faster fault detection in comparison with transmission of control packets. Enabling the echo function in asynchronous mode greatly reduces transmission of control packets because the detection is accomplished by the echo function. Enabling the echo function in query mode thoroughly cancels transmission of control packets after a session is established. The echo function must be enabled at both ends of a BFD session. Otherwise, the echo function does not take effect.

The echo mode includes the echo mode and one-armed echo mode. The one-armed echo mode is applicable to the single-hop IP link scenario and generally used in two directly connected devices, where one device supports the BFD function and the other does not. The echo mode requires that the echo mode be configured for both detection parties.

Specification

- The query mode is not supported and cannot be configured at present.
- Only BFD session version 1 supports the BFD echo mode.
- The echo mode is not supported for an IPv6 BFD session with the link-local address as the source or destination address.

1.1.4 BFD Support for Applications

By supporting BFD, the associated applications can utilize the fast fault detection of BFD to improve the protocol convergence performance. In general, the fault detection time can be shortened to less than 1 second. After BFD support for a certain application is enabled, BFD rapidly detects faults occurring on an established BFD session. When a link fault occurs, BFD can rapidly identify the fault and notify the associated application to process the fault, thereby improving its convergence. Currently, BFD supports the following applications:

1. BFD Support for RIP

After BFD support for the Routing Information Protocol (RIP) is enabled, RIP can utilize the faster fault detection feature of BFD than the hello mechanism of RIP to improve the protocol convergence. In general, the fault detection time can be shortened to less than 1 second.

Note

For more details about BFD support for RIP, see "Configuring RIP."

2. BFD Support for OSPF

After BFD support for OSPF is enabled, OSPF can utilize the faster fault detection feature of BFD than the hello mechanism of OSPF to improve the protocol convergence. In general, the fault detection time can be shortened to less than 1 second.

Note

For more details about BFD support for OSPF, see "Configuring OSPFv2."

3. BFD Support for OSPFv3

After BFD support for OSPFv3 is enabled, OSPFv3 can utilize the faster fault detection feature of BFD than the hello mechanism of OSPFv3 to improve the protocol convergence. In general, the fault detection time can be shortened to less than 1 second.

Note

For more details about BFD support for OSPFv3, see "Configuring OSPFv3."

4. BFD Support for BGP

After BFD support for Border Gateway Protocol (BGP) is enabled, BGP can utilize the faster fault detection feature of BFD than the hello mechanism of BGP to improve the protocol convergence. In general, the fault detection time can be shortened to less than 1 second.

Note

For more details about BFD support for BGP, see "Configuring BGP."

5. BFD Support for IS-IS

The Intermediate System to Intermediate System (IS-IS) protocol dynamically discovers neighbors through hello packets. After the BFD function is enabled on IS-IS, a BFD session is set up with a neighbor in up state. The BFD mechanism is used to detect the neighbor state. Once a neighbor failure is detected through BFD, IS-IS performs network convergence immediately. The convergence time can be reduced from 30s to less than 1s. By default, IS-IS hello packets are sent at an interval of **10** seconds in a P2P network, and the time required to detect a neighbor failure is three times the hello packet transmission interval.

Note

For more details about BFD support for IS-IS, see "Configuring IS-IS."

6. BFD Support for Static Routing

After BFD support for static routing is enabled, BFD prevents routers from selecting an unavailable static route as the forwarding path during routing and enables routers to rapidly switch to an available backup forwarding path. Different from dynamic routing protocols, static routing does not have the ND mechanism. Therefore, after BFD support for static routing is configured, the next-hop reachability of a static route relies on the BFD session state. If a BFD session detects a fault, the next hop of a static route is unreachable and the static route is not added to the routing information base (RIB). If the remote system deletes a BFD session during the establishment of the BFD session, the BFD session becomes down. In this case, the system ensures that the forwarding behavior of static routing is not affected.

Note

For more details about BFD support for static routing, see "Configuring Static Routing."

7. BFD Support for PBR

After BFD support for policy-based routing (PBR) is configured, BFD prevents routers from selecting an unavailable policy-based route as the forwarding path during routing and enables routers to rapidly switch to an available backup forwarding path. BFD support for PBR is equivalent to BFD support for static routing. BFD tracks and detects the forwarding path to a specified neighbor. When a BFD session fails, BFD notifies the PBR that the next hop is unreachable. Then, the policy-based route to the next hop does not take effect. If the remote system deletes a BFD session during the establishment of the BFD session, the BFD session becomes down. In this case, the system ensures that the PBR forwarding behavior is not affected.

Note

For more details about BFD support for PBR, see "Configuring PBR."

8. BFD Support for VRRP

The BFD support for the Virtual Router Redundancy Protocol (VRRP) can replace the hello mechanism of VRRP to rapidly detect the running status of the active and standby devices. When a fault occurs, it accelerates the active/standby device switching and improves network performance. In general, the fault detection time can be shortened to less than 1 second. VRRP can also utilize BFD to track a specified neighbor. If a BFD session detects that the forwarding path to the neighbor fails, VRRP automatically lowers the VRRP priority to a certain extent to trigger active/standby device switching. This configuration takes effect only when a dynamic routing protocol or other applications notify BFD to establish a session with a neighbor.

Note

For more details about BFD support for VRRP, see *Configuring VRRP*.

9. BFD Support for VRRP Plus

The BFD support for VRRP Plus can replace the balancing virtual forwarder (BVF) detection conducted by the balancing virtual gateway (BVG) of VRRP Plus to rapidly detect the running status of BVFs. When a fault occurs, it accelerates the forwarding entity switching and improves network performance. In general, the fault detection time can be shortened to less than 1 second. VRRP Plus is based on the VRRP protocol. Therefore, no additional configuration is required for BFD support for VRRP Plus and only VRRP needs to be enabled on devices at both ends and a BFD session is correctly associated.

Note

For more details about BFD support for VRRP Plus, see "Configuring VRRP Plus."

10. BFD Support for MPLS

The BFD support for Multiprotocol Label Switching (MPLS) enables label switched paths (LSPs) to use BFD to rapidly detect the neighbor status. The following detection modes are supported:

- BFD detects static LSPs.
- BFD detects LSPs generated by the Label Distribution Protocol (LDP).
- BFD detects reverse LSPs by using the IP addresses.

Note

For more details about BFD support for MPLS, see "MPLS Basics."

11. BFD Support for L3 Interfaces

BFD supports modifying the status of an L3 interface. In interface configuration mode, run the **bfdbindpeer-ip** command to detect the address of a specified directly connected L3 interface. After this CLI command is executed, a BFD session is created and the status of an L3 interface can be changed based on the detection result of the BFD session, for example, BFD Down or BFD Up. This function is often used in various types of fast reroute (FRR), which use BFD to detect the interface status to implement FRR switching.

Note

Only LDP FRR switching is supported when BFD support for L3 interfaces is configured.

12. BFD Support for AP Member Ports

After BFD support for aggregate port (AP) member ports is enabled, BFD can rapidly detect a fault occurring on a member port link so that traffic on this link is rapidly distributed to other effective member port links. In general, the fault detection time can be shortened to less than 1 second.

Note

For more details about BFD support for AP, see "Link Aggregation Port."

1.1.5 BFD Protection

If a BFD-enabled device is attacked (for example, attacked by a large number of ping packets), BFD sessions will flap. You can enable the BFD protection to provide protection. If both BFD and BFD protection are enabled on a device, the device discards the BFD packets received from the previous-hop device, which affects the establishment of a BFD session between the previous-hop device and other devices.

1.1.6 BFD Flapping Advertisement Dampening

A BFD session may frequently switch between the down and up states due to link instability. As a result, an associated application (such as static routing) may frequently switch forwarding paths, causing the frequent switching of the BFD session between the down and up states. This function allows users to set the delay for status change advertisement. After a BFD session is up for a certain period of time, BFD informs an associated application of BFD up. Otherwise, BFD informs it of BFD down.

1.1.7 SBFD Reflector Establishment

Compared with seamless bidirectional forwarding detection (SBFD), the BFD technology is relatively mature. However, when a large number of sessions are configured for link detection, the negotiation time of BFD's existing state machine becomes longer and turns into a bottleneck of the entire system. As a simplified mechanism of BFD, SBFD shortens the negotiation time. In large-scale commercial scenarios, SBFD implements faster communication fault detection and notifies the upper layer service in case of a fault. Like BFD sessions, SBFD sessions also distinguish different sessions through My Discriminator and Your Discriminator.

Since the reflector of SBFD does not perceive the detection service and is responsible for only looping back packets, only a reflector discriminator needs to be configured by running the **reflector discriminator** command at the reflector. This discriminator is Your Discriminator for the initiator. In a network, one initiator can be deployed to map to multiple reflectors, and multiple reflector discriminators can be configured for one reflector. All the reflector discriminators in the network must be globally unique.

1.1.8 Protocols and Standards

- draft-ietf-bfd-base-09: Bidirectional Forwarding Detection
- draft-ietf-bfd-generic-05: Generic Application of BFD
- draft-ietf-bfd-mib-06: Bidirectional Forwarding Detection Management Information Base
- draft-ietf-bfd-v4v6-1hop-09: BFD for IPv4 and IPv6 (Single Hop)
- draft-ietf-bfd-multihop-07: BFD for IPv4 and IPv6 (Multihop)
- draft-ietf-bfd-mpls-07: BFD For MPLS LSPs

Specification

Currently, draft-ietf-bfd-mib-06 and draft-ietf-bfd-multihop-07 are not supported.

1.2 Restrictions and Guidelines

- You are advised to keep the parameter configuration consistent at both ends of a BFD session. The purpose is to ensure that application protocols associated with BFD take effect simultaneously and prevent occurrence of one-way forwarding path due to different dampening time at both ends.
- Transmission bandwidth differences of different interfaces need to be taken into account during parameter configuration. If the configured minimum Tx interval and minimum Rx interval are very small, BFD may occupy excessive bandwidth and affect data transmission.
- BFD session parameters can be configured only after all the sessions on the current port complete negotiation. Otherwise, a configuration error is prompted. Run the **show bfd neighbors parm-consult** command to display the negotiation status of all the sessions.
- Ensure that BFD support is enabled on neighbors of a BFD session. Otherwise, a BFD session cannot be established. If a dynamic routing protocol or another application instructs BFD to establish a session with a neighbor, the BFD session can also be established.
- For a single-hop session whose source and destination IP addresses belong to the same network segment, if the interface specified by a BFD session is different from the actual BFD packet outbound interface because of IP routing, or if the interface specified during BFD session creation is different from the actual BFD packet inbound interface, a BFD session cannot be established. For a multi-hop session whose source and destination IP addresses belong to different network segments, associated applications do not need to specify an interface and BFD transmits and receives packets based on IP routing. Such BFD sessions can be established provided that returned BFD packets can be received.
- When BFD session traffic is sent and no BFD session parameters are configured on the device (the **show bfd neighbors** command shows that the number of BFD sessions is 0), the CPU protect policy (CPP) entries are not delivered. Therefore, the BFD traffic sent to the local device is not matched with the CPP entries and not sent to the local device. In this case, BFD sessions must be configured for sending the traffic

to the local device.

- In the process that the forwarding plane of the peer device returns echo packets transmitted by the local end to the local end, the echo packets may be lost due to congestion of the peer device, causing a session detection failure. In this case, you need to configure a quality of service (QoS) policy to ensure that echo packets are processed preferentially or disable the echo function.
- The echo detection function of BFD does not support multi-hop detection. Ensure that the echo function is disabled when configuring multi-hop detection.
- The echo mode takes effect only after it is enabled at both ends of a BFD session.
- Before enabling the echo mode of BFD, run the **no ip redirects** command on the neighbors of a BFD session to disable the function of sending Internet Control Message Protocol (ICMP) redirection packets, and run the **no ip deny land** command to disable the distributed denial of service (DDoS) function to prevent the land-based attack.

1.3 Configuration Task Summary

BFD configuration includes the following tasks:

(1) Configuring BFD Basic Functions

- Configuring BFD Parameters
- (Optional) Configuring the BFD Echo Mode
- (Optional) Configuring the BFD Slow Timer
- (Optional) Configuring BFD Support for L3 Interfaces
- Configuring BFD Support for Applications

(2) (Optional) Configuring BFD Protection

(3) (Optional) Configuring BFD Flapping Advertisement Dampening

(4) (Optional) Configuring an SBFD Reflector

1.4 Configuring BFD Basic Functions

1.4.1 Overview

You can establish BFD sessions and configure BFD support for applications to perform link fault detection.

1.4.2 Configuration Tasks

The basic function configuration of BFD includes the following tasks:

(1) Configuring BFD Parameters

(2) (Optional) Configuring the BFD Echo Mode

(3) (Optional) Configuring the BFD Slow Timer

(4) (Optional) Configuring BFD Support for L3 Interfaces

(5) Configuring BFD Support for Applications

1.4.3 Configuring BFD Parameters

1. Overview

- Unless otherwise specified, for single-hop sessions, a BFD session should be established between devices at both ends to be detected by BFD and BFD parameters must be configured at the egresses. Multi-hop sessions use global parameters for session establishment by default. If different negotiation parameters need to be configured for different multi-hop sessions, BFD templates need to be associated with the sessions.
- Transmission bandwidth differences of different interfaces need to be taken into account during parameter configuration. If the configured minimum Tx interval and minimum Rx interval are very small, BFD may occupy excessive bandwidth and affect data transmission.

2. Restrictions and Guidelines

- Negotiation parameters can be configured only after all the original sessions on a port complete negotiation.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure BFD parameters.

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*

No BFD session parameters are configured by default.

1.4.4 Configuring the BFD Echo Mode

1. Overview

- (Optional) Ports run in asynchronous mode by default. If a BFD session needs to run in echo mode, the echo mode needs to be configured. The echo mode includes the echo mode and one-armed echo mode.
- Complete the configuration on ports.
- A BFD session runs in asynchronous mode as long as either of devices at both ends is configured to run in asynchronous mode. If routers at both ends are configured to run in echo mode by default, a BFD session finally runs in echo mode. This function is disabled by default and can be enabled after the **bfd echo** command is executed.
- Run the **bfd echo one-arm** command to enable the one-armed echo mode.

2. Restrictions and Guidelines

By default, when BFD session parameters are configured, the system automatically enables the echo mode. To disable the BFD echo function, run the **no bfd echo** command in interface configuration mode. The minimum Tx interval and minimum Rx interval of echo packets adopt the **Interval milliseconds** and **min_rx milliseconds** parameters configured for a session.

Before enabling the echo mode of BFD, run the **no ip redirects** command on the neighbors of a BFD session to disable the function of sending ICMP redirection packets, and run the **no ip deny land** command to disable the DDoS function to prevent the land-based attack.

The BFD one-armed echo function and **ip redirect-drop** cannot be configured at the same time, otherwise the function fails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the BFD echo mode.

bfd echo [**one-arm**]

The echo mode is disabled for a BFD session by default.

1.4.5 Configuring the BFD Slow Timer

1. Overview

- The default slow timer is **3000** milliseconds. The value can be changed as required.
- Configure this function in global configuration mode.
- In BFD echo mode or during session establishment, control packets are sent based on the slow timer. A larger value indicates that the required time for negotiating and establishing a BFD session is longer and the time required for transmitting slow BFD packets in echo mode is longer.

2. Restrictions and Guidelines

This command is used to specify the slow timer in echo mode.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the BFD slow timer.

bfd slow-timer [*interval*]

The default slow timer time in the echo mode is **2000** milliseconds.

1.4.6 Configuring BFD Support for L3 Interfaces

1. Overview

- Currently, this function is used only when MPLS LDP is used for FRR switching.

- Complete the configuration on ports.

2. Restrictions and Guidelines

This command is used to enable BFD support for L3 interfaces so as to rapidly detect connectivity of L3 interfaces.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure BFD support for L3 interfaces.

bfd bind peer-ip *ipv4-address* [**source-ip** *ipv4-address*] **process-pst**

BFD support for interfaces is not configured by default.

1.4.7 Configuring BFD Support for Applications

1. Overview

- This function is disabled by default.
- The configuration command varies with the associated applications. For details, see their configuration guides.
- This function must be configured at both ends so that a BFD session can be established.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure BFD support.

bfd all interfaces

In RIP routing configuration mode, enable BFD support for RIP on all interfaces. For details, see "Configuring RIP."

bfd all interfaces

In OSPF routing configuration mode, enable BFD support for OSPF on all interfaces. For details, see "Configuring OSPFv2."

bfd all interfaces

In OSPFv3 routing configuration mode, enable BFD support for OSPFv3 on all interfaces. For details, see "Configuring OSPFv3."

neighbor *address* **fall-over bfd**

In BGP routing configuration mode, enable BFD support for BGP. For details, see "Configuring BGP."

bfd all interfaces

In IS-IS routing configuration mode, enable BFD support for IS-IS on all interfaces. For details, see "Configuring IS-IS."

Ip route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]

In global configuration mode, enable BFD support for static routing. For details, see "Configuring Static Routing."

ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv6-address*]

In global configuration mode, enable BFD support for static IPv6 routing. For details, see "Configuring Static Routing."

set ipnext-hopverify-availability next-hop-address **bfd** [**vrf** *vrf-name*] interface-type interface-number gateway

Enable BFD support for PBR. For details, see "Configuring PBR."

set ipv6 next-hopverify-availability *next-hop-address* **bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway*

Enable BFD support for IPv6 PBR. For details, see "Configuring PBR."

vrrp bfd *interface-type interface-number ip-address*

Enable BFD support for VRRP. For details, see "Configuring VRRP."

VRRP Plus is based on the VRRP protocol. Therefore, no additional configuration is required for BFD support for VRRP Plus and only VRRP needs to be enabled on devices at both ends and a BFD session is correctly associated.

bfd bind static-lsp peer-ip *ip-address* **source-ip** *ip-address* [**local-discriminator** *discr-value* **remote-discriminator** *discr-value*] [**process-state**]

Enable BFD support for static LSPs. For details, see "MPLS Basics."

bfd bind ldp-lsppeer-ip *ip-address* **nexthop** *ip-address* [**interface** *interface-type interface-number*] **source-ip** *ip-address* [**local-discriminator** *discr-value* **remote-discriminator** *discr-value*] [**process-state**]

Enable BFD support for LDP LSPs. For details, see "MPLS Basics."

bfd bind backward-lsp-with-ippeer-ip *ip-address* [**vrf** *vrf-name*] **interface** *interface-type interface-number* [**source-ip** *ip-address*] { **local-discriminator** *discr-value* **remote-discriminator** *discr-value*}

Enable BFD support for dynamic LSPs. For details, see *MPLS Basics*.

1.5 Configuring BFD Protection

1.5.1 Overview

- If a BFD-enabled device is attacked (for example, attacked by a large number of ping packets), BFD sessions flap. In this case, you can configure BFD protection to provide protection.

1.5.2 Restrictions and Guidelines

- The BFD basic functions must be configured.
- If both BFD and BFD protection are enabled on a device, the device discards the BFD packets received from the previous-hop device, which affects the establishment of a BFD session between the previous-hop device and other devices.

1.5.3 Prerequisites

Basic functions of BFD have been configured.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure BFD protection.

bfd cpp

Configure BFD protection on a device in the network where attacks exist.

The BFD protection is enabled by default.

1.6 Configuring BFD Flapping Advertisement Dampening

1.6.1 Overview

- A BFD session may frequently switch between the down and up states due to link instability. As a result, a relevant application (such as static routing) may frequently switch forwarding paths and the running services are affected.
- Users can set a delay for status change advertisement, after which BFD informs an associated application of BFD up. After a BFD session is up for a certain period of time, BFD informs an associated application of BFD up. Otherwise, BFD informs it of BFD down. This aims to reduce flapping of associated protocols caused by unstable links.

1.6.2 Restrictions and Guidelines

- The BFD basic functions must be configured.
- If a BFD session does not frequently switch between the down and up states, enabling BFD flapping advertisement dampening will delay notifying an associated application of BFD up.
- Enabling BFD flapping advertisement dampening can relieve frequent processing of associated applications (such as route re-calculation) caused by frequent advertisement of BFD status changes. The larger the configured time is, the longer the required BFD stability time is. BFD notifies an application module of BFD up only after the stability time reaches the configured time.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure flapping dampening parameters.

bfd up-dampening { *milliseconds* }

The BFD flapping advertisement dampening is disabled on ports by default. If a BFD session frequently switches between the down state and up state, you are advised to enable this function.

1.7 Configuring an SBFD Reflector

1.7.1 Overview

This section describes how to configure an SBFD reflector discriminator.

1.7.2 Restrictions and Guidelines

In a network, one initiator can be deployed to map to multiple reflectors, and multiple reflector discriminators can be configured for one reflector. All the reflector discriminators in the network must be globally unique.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an SBFD reflector.

sbfd reflector discriminator { *unsigned-integer-value* }

(4) Configure an SBFD reflector discriminator.

sbfd reflector discriminator

The reflector discriminator is Your Discriminator for the initiator.

1.8 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Caution

- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-2 BFD Monitoring

Command	Purpose
show bfd neighbors [**vrf** *vrf-name*] [**client** { **ap** | **bgp** | **ospf** | **rip** | **vrrp** | **static-route** | **pbr** | **vrrp-balance** | **ldp-lsp** | **static-lsp** | **backward-lsp-with-ip** | **pst**| **dhcp** | **openflow** | **pimdm** | **pimsm** | **pimsmv6** | **srp** }] [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*] [**details**] [**parm-consult** [*interface-type interface-number*]]	Displays BFD session information.
debug bfd event [**interface** *interface-type interface-number* **| ipv4** *ipv4-address* **| ipv6** *ipv6-address*]	Debugs BFD events.
debug bfd packet [**interface** *interface-type interface-number* **| ipv4** *ipv4-address* **| ipv6** *ipv6-address*]	Debugs BFD packets.

1.9 Configuration Examples

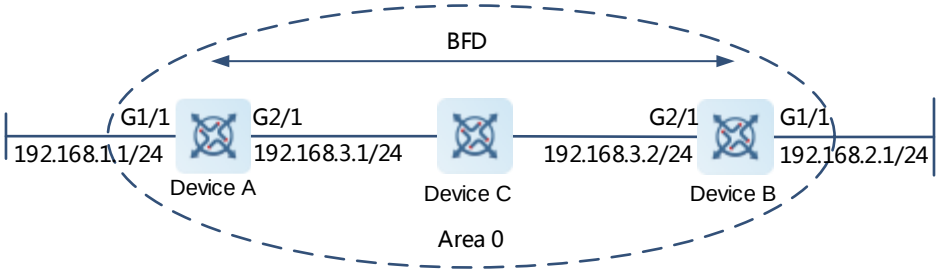
1.9.1 Configuring BFD Support for OSPF

1. Requirements

Three devices are used to build a network, the devices run the OSPF protocol, and BFD support for OSPF is enabled on two devices.

2. Topology

Figure 1-4 Topology for Configuring BFD Support for OSPF



3. Notes

- Configure IP addresses for ports connecting devices A and B.
- Run the OSPF protocol on devices A and B.
- Configure BFD parameters for the interconnected ports of devices A and B.
- Enable BFD support for OSPF on devices A and B.

4. Procedure

Perform the following configuration on device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet2/1
DeviceA(config-if-GigabitEthernet2/1)# no switchport
```

```
DeviceA(config-if-GigabitEthernet2/1)# ip address 192.168.3.1 255.255.255.0
DeviceA(config-if-GigabitEthernet2/1)# bfd interval 200 min_rx 200 multiplier 5
DeviceA(config-if-GigabitEthernet2/1)# exit
DeviceA(config)# interface GigabitEthernet1/1
DeviceA(config-if-GigabitEthernet1/1)# no switchport
DeviceA(config-if-GigabitEthernet1/1)# ip address 192.168.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet1/1)# exit
DeviceA(config)# router ospf 123
DeviceA(config-router)# log-adj-changes detail
DeviceA(config-router)# network 192.168.3.0 0.0.0.255 area 0
DeviceA(config-router)# network 192.168.1.0 0.0.0.255 area 0
DeviceA(config-router)# bfd all-interfaces
```

Perform the following configuration on device B.

```
DeviceB# configure terminal
DeviceB(config)# interface GigabitEthernet2/1
DeviceB(config-if-GigabitEthernet2/1)# no switchport
DeviceB(config-if-GigabitEthernet2/1)# ip address 192.168.3.2 255.255.255.0
DeviceB(config-if-GigabitEthernet2/1)# bfd interval 200 min_rx 200 multiplier 5
DeviceB(config-if-GigabitEthernet2/1)# exit
DeviceB(config)# interface GigabitEthernet1/1
DeviceB(config-if-GigabitEthernet1/1)# no switchport
DeviceB(config-if-GigabitEthernet1/1)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet1/1)# exit
DeviceB(config)# router ospf 123
DeviceB(config-router)# log-adj-changes detail
DeviceB(config-router)# network 192.168.3.0 0.0.0.255 area 0
DeviceB(config-router)# network 192.168.2.0 0.0.0.255 area 0
DeviceB(config-router)# bfd all-interfaces
```

5. Verification

Run the **show bfd neighbors details** command to check whether BFD support configuration is correct.

```
DeviceA# show bfd neighbors details
OurAddr       NeighAddr   LD/RD   RH/RS   Holdown(mult)   State   Int
192.168.3.1   192.168.3.2     1/2     Up      532 (3 )            Up      Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: OSPF
Uptime: 02:18:49
Last packet: Version: 1  - Diagnostic: 0
I Hear You bit: 1            - Demand bit: 0
Poll bit: 0              - Final bit: 0
```

```
Multiplier: 3            - Length: 24
My Discr.: 2             - Your Discr.: 1
Min tx interval: 50000       - Min rx interval: 50000
Min Echo interval: 0
```

```
DeviceB# show bfd neighbors details
OurAddr       NeighAddr   LD/RD   RH/RS   Holdown(mult)   State   Int
192.168.3.2   192.168.3.1 2/1     Up      532 (5 )            Up      Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago
Registered protocols: OSPF
Uptime: 02:18:49
Last packet: Version: 1  - Diagnostic: 0
I Hear You bit: 1            - Demand bit: 0
Poll bit: 0              - Final bit: 0
Multiplier: 5        - Length: 24
My Discr.: 1             - Your Discr.: 2
Min tx interval: 200000  - Min rx interval: 200000
Min Echo interval: 0
```

6. Common Errors

- For a single-hop session, BFD parameters may not be configured for the port on the device at one end of the session.
- If different negotiation parameters need to be configured for different multi-hop sessions, templates need to be associated with the sessions and negotiation parameters need to be configured in the templates.
- For multi-hop BFD sessions, if the sessions use different templates, negotiation parameters in the template used by a session that becomes up first are used for transmitting and receiving packets.
- BFD support for applications is not configured.
- BFD support for applications is enabled only on the device at one end.

Contents

1 Configuring Track 1
1.1 Introduction 1
1.1.1 Basic Concepts 1
1.1.2 ICMP Echo Test 1
1.1.3 UDP Echo Test 1
1.1.4 DHCP Test 2
1.1.5 TCP Test 2
1.1.6 DNS Test 2
1.1.7 Track Support for the RNS 3
1.2 Configuration Task Summary 4
1.3 Configuring Basic Features of RNS 4
1.3.1 Overview 4
1.3.2 Restrictions and Guidelines 4
1.3.3 Procedure 4
1.4 Configuring the ICMP Echo Test 5
1.4.1 Overview 5
1.4.2 Restrictions and Guidelines 5
1.4.3 Procedure 5
1.5 Configuring the DNS Test 6
1.5.1 Overview 6
1.5.2 Restrictions and Guidelines 6
1.5.3 Procedure 6
1.6 Configuring the TCP Connection Test 7

1.6.1 Overview 7

1.6.2 Restrictions and Guidelines 7

1.6.3 Procedure 7

1.7 Configuring the UDP Echo Test 8

1.7.1 Overview 8

1.7.2 Restrictions and Guidelines 8

1.7.3 Procedure 8

1.8 Configuring the DHCP Test 8

1.8.1 Overview 8

1.8.2 Restrictions and Guidelines 8

1.8.3 Procedure 8

1.9 Configuring the Track Support for the RNS 9

1.9.1 Overview 9

1.9.2 Restrictions and Guidelines 9

1.9.3 Procedure 9

1.10 Monitoring 10

1.11 Configuration Examples 11

1.11.1 Configuring the ICMP Echo Test 11

1.11.2 Configuring the DNS Test 12

1.11.3 Configuring the TCP Connect Test 13

1.11.4 Configuring the UDP Echo Test 14

1.11.5 Configuring the DHCP Test 15

1.11.6 Configuring to Track Link Status of an Interface 16

1.11.7 Configuring to Track the Status of Multiple Interfaces 17

1.11.8 Configuring to Track A Single RNS Instance 18

1.11.9 Configuring to Track the Results of Multiple RNS Instances 18

1 Configuring Track

1.1 Introduction

The reliable network service (RNS) tests the services provided by a peer device to monitor the service availability, integrity of the end-to-end connection, and service quality. With the RNS test results, you can learn the network performance in time and take measures accordingly to handle related network performance problems. Meanwhile, you can diagnose and locate network faults. The RNS test in this document is also called track test.

1.1.1 Basic Concepts

1. RNS Instance

An RNS instance can be treated as an RNS process. Before performing the RNS, you must create an RNS instance. In the RNS instance, you need to configure the RNS parameters, such as the test type, test destination address, and test frequency. The instance ID is globally unique.

2. RNS Test

RNS test aims to monitor the network connectivity, service availability, integrity of end-to-end connection, and service quality. For example, the RNS tests whether the domain name server (DNS) function of the device is normal. Currently, the RNS supports the following types of tests: RNS Test, DNS, TCP, UDP-Echo, and HTTP.

1.1.2 ICMP Echo Test

The Internet Control Message Protocol (ICMP) echo test is a basic function of the RNS, and is implemented in compliance with the RFC 2925. An ICMP packet is sent to check whether the destination is reachable and to calculate the network response time and packet loss rate.

An ICMP echo request packet is sent to the destination IP address based on the preset test time and frequency. Upon receipt of the ICMP echo request packet, an ICMP echo reply packet is returned from the destination IP address. Through the ICMP echo test, the response time and packet loss rate is calculated based on the information relating to the received ICMP echo reply packet, for example, the receipt time and number of packets. In this way, the current network performance and status are reflected. The ICMP echo test results and historical records are saved, and you can use the command line to display them.

Caution

The prerequisite for a successful ICMP echo test is that destination devices can correctly respond to ICMP echo request packets.

1.1.3 UDP Echo Test

User Datagram Protocol (UDP) echo is used to test the network accessibility and delay. When UDP packets are used to test the network accessibility and delay, the RNS server must be enabled on the peer end with the UDP port enabled, or the RNS server must be able to respond to ICMP port unreachable packets.

A UDP packet is sent to the destination IP address based on the preset test time and frequency. Upon receipt of the UDP packet, the device of the destination IP address replies by using such packet. Through the UDP echo test, the time required for packet round trip and packet loss rate are calculated based on the information relating to the received UDP packet from the server to reflect the current network performance and network conditions. The UDP echo test results and historical records are saved, and you can use the command line to display them.

1.1.4 DHCP Test

The Dynamic Host Configuration Protocol (DHCP) test is used to test the DHCP service function of the peer device and the network accessibility and delay. When DHCP packets are used to test the network accessibility and delay, the RNS service must be enabled on the peer end.

After the detection time and frequency are set, the DHCP test process is as follows:

1. The client sends a DHCP discovery packet to the test destination IP address, and the destination server replies with an offer packet after receiving the DHCP discovery detection packet.
2. After receiving the offer packet, the client replies with a request packet. The destination server receives the request packet and replies with an ack packet.
3. After receiving the ack packet, the client deems that the detection succeeds, and sends a cancel packet to the server.

The detection client calculates the time required for the client to obtain the IP address and the packet loss rate according to the information of the received DHCP ack packet, reflecting the current network performance and network conditions. The DHCP test results and historical records are saved. You can run the **show ip rns configuration** command to view them.

1.1.5 TCP Test

The Transmission Control Protocol (TCP) test is used to test the availability of a TCP connection. A TCP connection can be established based on the configured destination IP address and port ID. If the TCP connection is established successfully, the test succeeds; otherwise, the test fails.

1.1.6 DNS Test

In a DNS test, a DNS client is simulated to send a domain name resolution request to a specified DNS server. You can determine whether the DNS server is available and the domain name resolution speed by checking the domain name resolution result and the time required for domain name resolution. In the DNS test, the domain name resolution process is simulated, and the mapping between the resolved domain name and the IP address is not saved. The DNS test results and historical records are saved in the test group. You can use the command line to view them.

The procedure for configuring an RNS instance test is as follows:

(1) Create an instance and configure the test based on the test type.

(2) Start the instance.

(3) Use the RNS instance to construct a packet of the specific test type and send the packet to the peer end.

(4) Upon receipt of the test packet, the peer end returns a reply packet of the corresponding type.

(5) The RNS instance calculates the packet loss rate and round trip time based on whether a reply packet is received and the time of reply packet receipt.

(6) Run the **show** or **debug** command to view the test result.

1.1.7 Track Support for the RNS

Objects that can be tracked include: the test result of an RNS instance, RNS list status, link status on an interface, and track list status. When the track status changes, an action of other modules is triggered. The working process of track is described below by taking different track objects as examples.

- Configure a track object for tracking the test result of an RNS instance.
  - When the test result of the RNS instance changes, the RNS module sends a status change message to the track module.
  - The track module receives the test result. After the preset delay, if the test result remains unchanged, the status of the track object is modified, and the module of the track object is notified of the modification. If the test result recovers within the period, the status of the track object is not modified and the corresponding module is not notified.
- Configure a track object for tracking the link status of an interface.
  - If the link status of the interface is up, the status of the track object is also up.
  - If the link status of the interface is down, the status of the track object is also down.
- Configure a track object for tracking the test result of an RNS instance.
  - If the RNS test succeeds, the status of the track object is also up.
  - If the RNS test fails, the status of the track object is also down.
- Configure a track object for tracking the test result of an RNS list.
  - The result can be the AND or OR operation result of all member status.
  - If the result of this track object is set to the AND operation result of all member status, and the AND result of the status of all the track RNS objects is up, the status of this track object is up. So long as the RNS test result of one track RNS object is down, the status of this track object is also down.
  - If the result of this track object is set to the OR operation result of all member status, and the OR result of the status of all the track RNS objects is down, the status of this track object is down. So long as the RNS test result of one track RNS object is up, the status of this track object is also up.
- Configure a track object for tracking the status of a track list.
  - Set the result of the track object to the AND operation result of all member status.
  - When the AND operation result of all member status is up, the status of this track object is also up.
  - When the AND operation result of all member status is down the status of this track object is also down.
- Configure a track list member.

  Configure a track list member. The status of the member can be the same as or contrary to that of the corresponding track object.
- Adjust the delay for notifying the status change of a track object.
  - A longer delay indicates that it takes more time before the module that is concerned with the track object is informed of the status.
  - A shorter delay indicates that it takes less time before the module that is concerned with the track object is informed of the status.

1.2 Configuration Task Summary

RNS configuration includes the following tasks:

(1) Configuring Basic Features of RNS

(2) Configuring the ICMP Echo Test

(3) Configuring the DNS Test

(4) Configuring the TCP Connection Test

(5) Configuring the UDP Echo Test

(6) Configuring the DHCP Test

(7) Configuring the Track Support for the RNS

1.3 Configuring Basic Features of RNS

1.3.1 Overview

Configure details of an RNS test instance to complete basic configuration of the RNS instance. Brief configuration is also available. Configure and start an RNS instance at a time.

1.3.2 Restrictions and Guidelines

- In detailed configuration mode, if you do not configure the test type after entering the IP RNS mode by running the command, the RNS instance is not created.
- In detailed configuration mode, after configuring an RNS instance, you need to run the **ip rns schedule** command to configure the startup policy; otherwise, the test is not implemented.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Define an RNS operation object.

ip rns *operation-number* [{ **dns** *destination-hostname* **name-server** *ipv4-address* | **icmp-echo** *destination-ipv4-address* | **tcp-connect** *destination-ipv4-address port-number* } [**frequency** *interval*] [**timeout** *interval*] [**threshold** *interval*]]

No track operation object is created by default.

(4) Configure the proactive threshold monitoring and triggering mechanism of the RNS test.

ip rns reaction-configuration *operation-number* **react** { **allfail** | **rtt** | **timeout** } [**action-type track**] [**threshold-type** { **average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*] }] [**threshold-value** *max-threshold min-threshold*]

The proactive threshold monitoring and triggering mechanism is not configured for the test by default.

(5) Enable an RNS instance to trigger another RNS instance.

ip rns reaction-trigger *source-operation-number target-operation-number*

The trigger mechanism when the monitoring threshold exceeds the expectation is not configured for the test by default.

(6) Configure scheduling parameters of an RNS instance.

ip rns schedule *operation-number* [**life** { **forever** | *period* }] [**start-time** { *hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss* }] [**recurring**]

No scheduling policy is configured for the test by default.

(7) Configure the **ip rns restart** command to restart an RNS instance.

ip rns restart *operation-number*

To restart an IP RNS instance in pending status of scheduling, perform this configuration (or directly configure scheduling start: **ip rns schedule** *operation-number* **start-time now**).

The test restart function is not configured by default.

(8) Run the **ip rns reset** command to clear the RNS test configuration.

ip rns reset

Perform this configuration if you need to clear configurations of all the RNS instances, for example, when a lot of instances are configured but configuration errors are found.

The RNS test clearing function is not configured by default.

(9) Configure the **ip rns server** command to enable the server function.

ip rns-server udp-echo *port-number*

This configuration is mandatory when you need to enable the RNS server for UDP echo tests.

The server function of UDP echo test is not configured by default.

1.4 Configuring the ICMP Echo Test

1.4.1 Overview

Create an RNS test instance of ICMP echo type.

1.4.2 Restrictions and Guidelines

You must first configure the RNS basic features.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Create an RNS test instance of ICMP echo type.

icmp-echo { **oob** { *destination-ipv4-address* | *destination-hostname* [**name-server** *ipv4-address*] } [**source-ipaddr** *ipv4-address*] **via** *interface-type interface-number* **next-hop** *ipv4-address* } |

{ { *destination-ipv4-address* | *destination-hostname* [**name-server** *ipv4-address*] } [**source-ipaddr** *ipv4-address* | **source-interface** interface-type interface-number] [[**af-direct**] **out-interface** *interface-type interface-number* [**next-hop** *ipv4-address*]] }

icmp-echo { *destination-ipv4-address* | *destination-hostname* [**name-server** *ipv4-address*] } [**source-ipaddr** *ipv4-address* | **source-interface** *interface-type interface-number*] [

[**af-direct**] **out-interface** *interface-type interface-number* [**next-hop** *ipv4-address*]]

No test of ICMP echo type is created by default.

(5) (Optional) Configure the repeat test interval.

frequency *interval*

The default test interval is **60** seconds.

(6) (Optional) Configure the tag parameter.

tag *tag-name*

No test tag is configured by default.

(7) (Optional) Configure the time threshold parameter.

threshold *interval*

The default upper threshold of test is **5** seconds.

(8) (Optional) Configure the timeout period.

timeout *interval*

The default timeout interval of a test is **5** seconds.

(9) (Optional) Configure the type of service (TOS) parameter.

tos *tos-values*

The default TOS value for IPv4 packet of the test is **0**.

(10) (Optional) Configure the virtual routing and forwarding (VRF) of an RNS test.

vrf *vrf-name*

No VRF name is configured for the test by default.

(11) Configure the protocol payload size for the test.

request-data-size *bytes*

The default protocol payload size is **36** bytes for the tests of ICMP echo and UDP echo types.

1.5 Configuring the DNS Test

1.5.1 Overview

Create an RNS test instance of DNS type.

1.5.2 Restrictions and Guidelines

You must first configure the RNS basic features.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an RNS test instance of DNS type.

dns { **oob** *destination-hostname* **name-server** *ipv4-address* [**source-ipaddr** *ipv4-address*] **via** *interface-type interface-number* **next-hop** *ipv4-address* } | { *destination-hostname* **name-server** *ipv4-address* [**source-ipaddr** *ipv4-address*] [[**af-direct**] **out-interface** *interface-type interface-number* [**next-hop** *ipv4-address*]] }

dns *destination-hostname* **name-server** *ipv4-address* [**source-ipaddr** *ipv4-address*] [[**af-direct**] **out-interface** *interface-type interface-number* [**next-hop** *ipv4-address*]]

No test of DNS type is created by default.

Caution

For the commands (**frequency, tag, threshold, timeout, and tos**) of configuring common optional parameters of a test, see 1.4 Configuring the ICMP Echo Test. They are omitted here.

1.6 Configuring the TCP Connection Test

1.6.1 Overview

Create an RNS test instance of TCP type to implement a TCP connection test.

1.6.2 Restrictions and Guidelines

- You must first configure the RNS basic features.
- The target host must be able to respond to the TCP connection request.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an RNS test instance of TCP type.

tcp-connect { *destination-ipv4-address* | *destination-hostname* [**name-server** *ipv4-address*] } *port-number* [**source-ipaddr** *ipv4-address*] [[**af-direct**] **out-interface** *interface-type interface-number* **next-hop** *ipv4-address*]

No test of TCP type is configured by default.

Caution

For the commands (**frequency, tag, threshold, timeout, and tos**) of configuring common optional parameters of a test, see 1.4 Configuring the ICMP Echo Test. They are omitted here.

1.7 Configuring the UDP Echo Test

1.7.1 Overview

Create an RNS test instance of UDP echo type and implement the UDP echo test.

1.7.2 Restrictions and Guidelines

- You must first configure the basic features of the RNS and RNS server.
- The RNS server must be enabled to provide server functions.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an RNS test instance of UDP echo type.

udp-echo { **oob** *destination-ipv4-address port-number* [**via** *interface-type interface-number* **next-hop** *next-hop-ip*] | *destination-ipv4-address port-number* [**out-interface** *interface-type interface-number* **next-hop** *next-hop-ip*] }

udp-echo *destination-ipv4-address port-number* [**out-interface** *interface-type interface-number* **next-hop** *next-hop-ip*]

No test object of UDP echo type is configured by default.

Caution

For the commands (**frequency, tag, threshold, timeout, and tos**) of configuring common optional parameters of a test, see *1.4 Configuring the ICMP Echo Test*. They are omitted here.

1.8 Configuring the DHCP Test

1.8.1 Overview

Create an RNS test instance of DHCP type to implement a DHCP test.

1.8.2 Restrictions and Guidelines

You must first configure the basic features of RNS and the IP address of the outbound port.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an RNS test instance of DHCP type.

dhcp *destination-ipv4-address* **out-interface** *out-interface* **next-hop** *next_ip_address*

Caution

For the commands (**frequency, tag, threshold, timeout, and tos**) of configuring common optional parameters of a test, see 1.4 Configuring the ICMP Echo Test. They are omitted here.

1.9 Configuring the Track Support for the RNS

1.9.1 Overview

Configure track support for RNS, including the test results of track RNS, the link status of the interface, the status of track list, and the status of RNS test list.

1.9.2 Restrictions and Guidelines

- To configure the track function to track the test result of an RNS instance, you need to configure the related RNS instance.
- To configure the track function to track the link status of an interface, you need to configure the related interface.
- To configure the track function to track the status of a track list, you need to configure the members for the related track list.
- To configure the track function to track the status of an RNS list, you need to configure the members for the related RNS list.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the track object. Select at least one of the following to configure.

- Configure to track the link status of an interface.

track *object-number* **interface** *interface-type interface-number* **line-protocol**

- Configure to track the RNS test result.

track *object-number* **rns** *entry-number*

- Configure to track the status of a track list.

track *object-number* **list boolean** { **and** | **or** }

- Configure to track the status of an RNS list.

track *object-number* **rns-list** *men-list* { **and | or** }

(5) Configure the notification delay of a track object.

delay { **up** *interval* [**down** *interval*] **|** [**down** *interval*] **up** *interval* }

Configure the delay for notifying the tracking status change from up to down or from down to up, or configure both at the same time.

No delay is set by default for notifying the track object status change from up to down or from down to up.

(6) Configure a track member.

object *object-number* [**not**]

No member object is configured by default.

1.10 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

Run the **debug** command to display debugging information.

Caution

- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 RNS Monitoring

Command	Purpose
show ip rns configuration [*operation-number*]	Displays the configuration of one or more RNS instances.
show ip rns collection-statistics [*operation-number*]	Displays the detailed statistics of one or more RNS instances.
show ip rns operational-state [*operation-number*]	Displays the current status of one or more RNS instances.
show ip rns-server udp-echo	Displays the RNS server configuration.
show ip rns reaction-configuration [*operation-number*]	Displays the proactive threshold monitoring information of one or more RNS instances.
show ip rns reaction-trigger [*operation-number*]	Displays information about the test triggered by one or more RNS instances.
show ip rns statistics [*operation-number*]	Displays the brief statistics of one or more RNS instances.
show track [*object-number*]	Displays the statistics of one or more track objects.
show track client	Displays the statistics of a track client.
debug track { **all | proc-event | rdnd-event | client** }	Debugs the track module.

Command	Purpose
debug rns { **all | interface | lib | rdnd-event | restart | rns_id** [**0, 500**] }	Debugs the RNS module.
debug rns-server {udp-echo} { event | fail | packet }	Debugs the RNS server module.

1.11 Configuration Examples

1.11.1 Configuring the ICMP Echo Test

1. Requirements

Configure an RNS test of ICMP echo type, which must be started immediately and take effect permanently.

2. Topology

Figure 1-1 Topology for Configuring the ICMP Echo Test

3. Notes

Configure RNS instance 1 and related parameters on Device A.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip rns 1
DeviceA(config-ip-rns)# icmp-echo 10.2.2.2
DeviceA(config-ip-rns-icmp-echo)# exit
DeviceA(config)# ip rns schedule 1 start-time now life forever
```

5. Verification

Run the **show ip rns configuration** command to display the instance configuration.

```
DeviceA# show ip rns configuration 1
Entry number: 1
Tag:
Type of operation to perform: icmp-echo
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 60000
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
```

```
Life (seconds): foerver
Next Scheduled Start Time:Start Time already passed
Target address/Source address: 10.2.2.2/0.0.0.0
Request size (ARR data portion): 36
```

1.11.2 Configuring the DNS Test

1. Requirements

Configure an RNS test of DNS type, which must be started immediately and take effect permanently.

2. Topology

Figure 1-2 Topology for Configuring the DNS Test

3. Notes

Configure RNS instance 1 and related parameters on Device A.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip rns 1
DeviceA(config-ip-rns)# dns www.abc.com name-server 10.2.2.2
DeviceA(config-ip-rns-dns)# exit
DeviceA(config)# ip rns schedule 1 start-time now life forever
```

5. Verification

Run the **show ip rns configuration** command to display the instance configuration.

```
DeviceA# show ip rns configuration 1
Entry number: 1
Tag:
Type of operation to perform: dns
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 60000
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
Life (seconds): foerver
Next Scheduled Start Time:Start Time already passed
Target host name: www.abc.com
Name Server: 10.2.2.2
```

6. Common Errors

The DNS IP address is incorrect.

1.11.3 Configuring the TCP Connect Test

1. Requirements

Configure an RNS test of TCP type, which must be started immediately and take effect permanently.

2. Topology

Figure 1-3 Topology for Configuring the TCP Connect Test

3. Notes

Configure RNS instance 1 and related parameters on Device A.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip rns 1
DeviceA(config-ip-rns)# tcp-connect 10.2.2.2 8000
DeviceA(config-ip-rns-tcp)# exit
DeviceA(config)# ip rns schedule 1 start-time now life forever
```

5. Verification

Run the **show ip rns configuration** command to display the instance configuration.

```
DeviceA# show ip rns configuration 1
Entry number: 1
Tag:
Type of operation to perform: tcp-connect
Operation timeout (milliseconds): 5000
Operation frequency (millseconds): 60
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
Life (seconds): foerver
Next Scheduled Start Time:Start Time already passed
Target Address: 10.2.2.2
Target Port: 8000
```

6. Common Errors

- The target host does not respond to the TCP connection request.
- The configured TCP port for the RNS test is incorrect.

1.11.4 Configuring the UDP Echo Test

1. Requirements

Configure an RNS test of UDP echo type, which must be started immediately and take effect permanently.

2. Topology

Figure 1-4 Topology for Configuring the UDP Echo Test

3. Notes

Configure RNS instance 1 and related parameters on Device A.

4. Procedure

Perform the following configuration Device A:

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip rns 1
DeviceA(config-ip-rns)# udp-echo 10.2.2.2 1025
DeviceA(config-ip-rns-udp-echo)# exit
DeviceA(config)# ip rns schedule 1 start-time now life forever
```

Perform the following configuration on Device B:

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip rns-server udp-echo 1025
```

5. Verification

Run the **show ip rns configuration** command to display the instance configuration.

```
DeviceA# show ip rns configuration 1
Entry number: 1
Tag:
Type of operation to perform: udp-echo
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 60000
Threshold (milliseconds): 5000
Target Address: 10.2.2.2
Target Port: 1025
Request size (ARR data portion): 36
```

Run the **show ip rns-server udp-echo** command to display the RNS server configuration.

```
DeviceA# show ip rns-server udp-echo
   UDP-Echo-Server:10000
   Receive packets number: 0
```

```
    Reflect packets success number: 0
    Reflect packets fail number: 0
```

6. Common Errors

The UDP server port configured on the client is not correct.

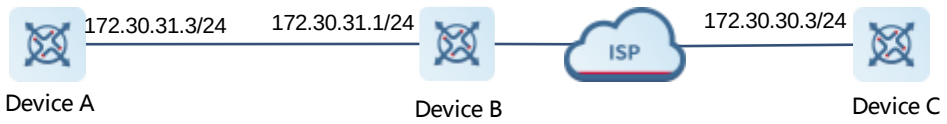
1.11.5 Configuring the DHCP Test

1. Requirements

Configure an RNS test of DHCP type, which must be started immediately and take effect permanently.

2. Topology

Figure 1-5 Topology for Configuring the DHCP Test



3. Notes

Configure RNS instance 1 and related parameters on Device A.

4. Procedure

Perform the following configuration on Switch A:

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip rns 1
DeviceA(config-ip-rns)# dhcp 172.30.30.3 out-interface GigabitEthernet 1/0/1 next-hop
172.30.31.1
DeviceA(config-ip-rns-dhcp)# exit
DeviceA(config)# ip rns schedule 1 start-time now life forever
```

5. Verification

Run the **show ip rns configuration** command to display the instance configuration.

```
DeviceA# show ip rns configuration 1
Entry number: 1
Tag:
Type of operation to perform: dhcp
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 60000
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
Life (seconds): forever
Next Scheduled Start Time: Start Time already passed
Target address/Source address: 172.30.30.3/172.30.31.252
Out-interface: GigabitEthernet 1/0/1
```

```
Next-hop address: 172.30.31.1
```

6. Common Errors

- The DHCP service is not enabled on the server.
- No IP address is configured for the outbound interface of the client.

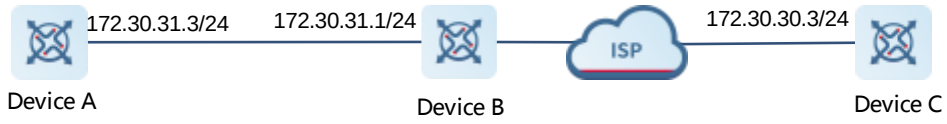
1.11.6 Configuring to Track Link Status of an Interface

1. Requirements

Configure track object 3 to track the link status of the interface GigabitEthernet 0/1.

2. Topology

Figure 1-6 Topology for Configuring to Track the Link Status of an Interface



3. Notes

- Configure a track object to track the link status of an interface.
- Configure the delay for notifying the status change from up to down.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# track 3 interface gigabitethernet 0/1 line-protocol
DeviceA (config-track)# delay down 10
```

5. Verification

Disable the interface GigabitEthernet 0/1, namely, change the link status to down. Immediately check the status of the track object, and verify that the status is still up. Check the status of the track object 10s later, and verify that the status changes to down.

```
DeviceA# show track 3
Track 3
  Interface GigabitEthernet 0/1
  The state is Up, delayed Down (5 secs remaining)
    1 change, current state last: 300 secs
  Delay up 0 secs, down 10 secs
```

6. Common Errors

- The track object for tracking an RNS test is configured, but the RNS test is not configured.
- The track object for tracking the link status of an interface is configured, but the corresponding interface is not configured.

- The track object for tracking the status of a track list is configured, but no member of the RNS list is configured.
- The track object configured for tracking an RNS list is configured, but the RNS test is not configured.

1.11.7 Configuring to Track the Status of Multiple Interfaces

1. Requirements

Configure track object 3. When track object 1 is up and object 2 is down, track object 3 is up.

2. Topology

Figure 1-7 Topology for Configuring to Track the Status of Multiple Interfaces

3. Notes

- Configure track objects 1 and 2.
- Configure track object 3, and its members include track objects 1 and 2.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA# config
DeviceA(config)# track 1 interface gigabitEthernet 0/0 line-protocol
DeviceA(config-track)# delay up 20 down 40
DeviceA(config-track)# exit
DeviceA(config)# track 2 interface gigabitEthernet 0/1 line-protocol
DeviceA(config-track)# delay down 30
DeviceA(config-track)# exit
DeviceA(config)# track 3 list Boolean and
DeviceA(config-track)# object 1
DeviceA(config-track)# object 2 not
```

5. Verification

```
DeviceA# show track 3
Track 3
  List boolean and
  Object 1
  Object 2 not
  The state is Down
    1 change,current state last:10 secs
  Delay up 0 secs,down 0 secs
```

1.11.8 Configuring to Track A Single RNS Instance

1. Requirements

Configure track object 5 to track the test result of RNS instance 7.

2. Notes

- Configure an RNS test.
- Configure a track object for tracking the test result of an RNS instance.
- Configure the delay for notifying the test result change from up to down and the delay for notifying the test result change from down to up.

3. Procedure

Perform the following configuration on Device A:

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip rns 7
DeviceA(config-ip-rns)# icmp-echo 2.2.2.2
DeviceA(config-ip-rns-icmp-echo)# exit
DeviceA(config)# ip rns schedule 7 start-time now life forever
DeviceA(config)# track 5 rns 7
DeviceA(config-track)# delay up 20 down 30
```

4. Verification

Make the test result of RNS instance 7 change from successful to unsuccessful. When the test result changes to unsuccessful, immediately check the status of track object 7, and verify that the status is still up. Check the status of the track object 30s later, and verify that the status changes to down.

```
DeviceA# show track 5
Track 5
  Reliable Network Service 7
  The state is Down
    2 change, current state last: 10 secs
  Delay up 20 secs, down 30 secs
```

1.11.9 Configuring to Track the Results of Multiple RNS Instances

1. Requirements

Configure track object 5 for tracking the test results of an RNS list (consisting of RNS instances 1, 2-5, and 8).

2. Notes

- Configure and start an RNS test.
- Configure a track object for tracking the test result of an RNS list.
- Configure the delay for notifying the test result change from up to down, and the delay for notifying the test result change from down to up.

3. Procedure

Perform the following configuration on Device A:

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# track 5 rns-list 1,2-5,8 and
DeviceA(config-track)# delay up 20 down 30
```

4. Verification

Make the test result of one of the RNS instances 1, 2-5, and 8 change from successful to unsuccessful. When the test result changes to unsuccessful, immediately check the status of track object 7, and verify that the status is still up. Check the status of the track object 30s later, and verify that the status changes to down.

```
DeviceA# show track 5
Track 5
  rns-list 1,2-5,8 and
  The state is Down
    2 change, current state last: 10 secs
Delay up 20 secs, down 30 secs
```

Contents

1 Configuring IP Event Dampening 1
1.1 Introduction 1
1.1.1 Basic Concepts 1
1.1.2 Protocols and Standards 2
1.2 Restrictions and Guidelines 2
1.3 Configuring IP Event Dampening 2
1.3.1 Overview 2
1.3.2 Restrictions and Guidelines 2
1.3.3 Procedure 2
1.4 Monitoring 3
1.5 Configuration Examples 3
1.5.1 Configuring IP Event Dampening 3

1 Configuring IP Event Dampening

1.1 Introduction

When an L3 network interface frequently goes Up or Down due to manual enabling/disabling or other external causes, the routing table on the device flaps repeatedly. If a routing protocol is configured, the protocol may extend the flap to the entire network, causing repeated updates and recalculation of neighboring routes. As a result, this wastes network bandwidth and destabilizes the network. Repeated route updates and recalculation on devices consume many CPU resources, and thus affect the normal running of customer networks.

The function of IP Event Dampening detects abnormal Up/Down flapping and automatically suppresses frequent interface state changes, which prevents a routing protocol from propagating single-point link failures. When an interface is restored to stable, it is automatically released, thus reducing network flaps and CPU resource consumption while improving network stability.

1.1.1 Basic Concepts

1. Penalty

IP Event Dampening uses the penalty method to perceive and control interface changes. Whenever an interface goes Up or Down, the penalty accumulates, but when the interface is stable, the penalty decreases exponentially. In this way, interface behaviors can be sensed and processed intelligently.

2. Suppress threshold

To identify an interface flap event, the function of IP Event Dampening configures a suppress threshold. When the cumulative penalty of an interface exceeds a suppress threshold, the interface is considered to flap and is suppressed.

3. Half-life period

The half-life period is the period for the penalty to decrease to half of the original value when an interface becomes stable. It defines the speed at which the penalty decays exponentially. The shorter the half-life period, the faster the penalty decays, and the faster the interface is detected to be stable, but the flap detection sensitivity is reduced more greatly.

4. Reuse threshold

When an interface does not flap and its penalty decays to a certain degree (below the suppress threshold), the interface is considered to be stable and is released.

5. Maximum suppress time

When an interface keeps flapping and reaches a very large penalty, the interface is not usable for a long time. To avoid this problem, we define the maximum suppress time to ensure that the interface suppression duration is less than the maximum suppress time no matter how long the interface has flapped.

6. Interface flap suppression

- An interface configured with IP Event Dampening is assigned a penalty. The interface gets a penalty of 1000 whenever it goes Down, and the penalty decreases with time. If the interface goes Down again, the penalty

increases. When the cumulative penalty exceeds the suppress threshold, the interface is suppressed. For the affected upper-layer protocol, the suppressed interface is always Down regardless of the interface state. When the penalty decreases to the reuse threshold, the interface is released and restored to its real state.

- If an L3 interface is not configured with IP Event Dampening or is not suppressed, the routing protocol or other protocols concerned about the interface state still work normally. When the interface is configured with IP Event Dampening and is suppressed, the upper-layer protocol considers the interface to be Down. During this process, any state change of the interface does not affect the routing table or the route calculation and advertisement performed by the upper-layer routing protocol until the interface is released.

1.1.2 Protocols and Standards

- RFC 2439: BGP Route Flap Damping

Note

The suppression algorithm core used by IP Event Dampening is the same as that used by Border Gateway Protocol (BGP) Route Flap Dampening stipulated in RFC 2439.

1.2 Restrictions and Guidelines

- The function of IP Event Dampening is supported only on L3 interfaces.

1.3 Configuring IP Event Dampening

1.3.1 Overview

When an interface configured with IP Event Dampening keeps flapping until the predefined threshold is exceeded, the interface is set to Down.

1.3.2 Restrictions and Guidelines

- When an L3 interface on a device is converted into an L2 interface, the IP Event Dampening command configured on the interface is deleted.
- IP Event Dampening cannot be configured on **virtual templates**.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Switch the interface mode.

no switchport

(5) Configure the function of IP Event Dampening.

dampening [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [**restart** [*restart-penalty*]]]]

The function of IP Event Dampening is disabled on an interface by default.

1.4 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Run the **debug** commands to output debugging information.

Caution

- Running the **clear** command during operation of the device may lose vital information and interrupt services.
- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
clear counters	Clears interface statistics.
show dampening interface	Displays statistics about interfaces with IP Event Dampening.
show interfaces [*interface-type interface-number*] **dampening**	Displays IP Event Dampening configurations.
debug dampening interface	Debugs IP Event Dampening.

1.5 Configuration Examples

1.5.1 Configuring IP Event Dampening

1. Requirements

Configure IP Event Dampening on L3 interfaces.

2. Topology

Figure 1-1 Configuring IP Event Dampening

3. Notes

- Enable IP Event Dampening on interface GigabitEthernet 0/1 on Device A and Device B respectively, and set the half-time period to 30s, the reuse threshold to 1500, the suppress threshold to 10,000, and the maximum suppress time to 120s.

4. Procedure

Configure IP Event Dampening on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# dampening 30 1500 10000 100
```

Configure IP Event Dampening on Device B.

```
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# dampening 30 1500 10000 100
```

5. Verification

Run the **show interfaces dampening** command to display the detailed information about Event Dampening on an interface.

```
DeviceA# show interfaces dampening
GigabitEthernet 0/1
  Flaps Penalty Supp    ReuseTm HalfL   ReuseV  SuppV   MaxSTm  MaxP    Restart
  0     0       FALSE   0       30      1500    1000    100     15119   0
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 no switchport
 dampening 30 1500 10000 100
!
end
```

- Device B configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 no switchport
 dampening 30 1500 10000 100
!
end
```

7. Common Errors

- IP Event Dampening is configured for an interface on an L3 device before the interface is converted to a routed interface by running the **no swithport** command.

Contents

1 Configuring HAM 1

1.1 Introduction 1

1.2 HAM Application 1

1.2.1 Detection Process 1

1.3 Configuring the HA Service of One Frequently Restarting Process 1

1 Configuring HAM

1.1 Introduction

High availability module (HAM) is a self-developed system high availability (HA) technology. It monitors exceptional exit of software processes of a device to automatically start the processes or monitors frequent restart of a software process to automatically restart the device, thus quickly and automatically restore services. Used during patch upgrade, this function can prevent device reset due to patch upgrade exceptions.

1.2 HAM Application

HAM is mainly used for:

- Software process HA service: When a software process exits abnormally, HAM automatically starts the software process to restore services.
- Device restart service: When a software process restarts frequently, HAM attempts to automatically restart the device to restore services.

Typically, the HA service of one frequently restarting process is enabled on all devices. You can run command line interface (CLI) commands on the master device to enable/disable this service and synchronize the service status to other non-master devices. During a patch upgrade, a process may restart due to an abnormal process. If the device automatically restarts, traffic may be interrupted. Therefore, you must disable the HA service of one frequently restarting process. After a patch upgrade, you can enable the HA service of one frequently restarting process when confirming that no process restarts frequently.

Caution

If you disable the HA service of one frequently restarting process by running a command, services may not automatically be restored to normal because some processes frequently restart due to no automatic restarting of the device. As a result, failure time prolongs.

1.2.1 Detection Process

HAM monitors kernel advertisements to perceive the status of an abnormal process and automatically restores services based on the following rules:

- If one process exits five times within two minutes, HAM attempts to start the process five minutes later.
- If a process restarts twice within 10 minutes, services cannot be restored. In this case, you must restart the device to restore them.

1.3 Configuring the HA Service of One Frequently Restarting Process

1. Overview

When one process exits abnormally, you can automatically restore services by configuring the HA service of one process that restarts frequently. You can further determine the exception to check whether the device needs to be restarted to restore services.

2. Restrictions and Guidelines

If one process frequently restarts, disabling its HA service may lead to a longer failure time. Therefore, you are advised to enable the configuration in scenarios other than patch upgrades.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Disable the HA service of one frequently restarting process.

no ham single-process-ha auto-restart enable

The HA service of one frequently restarting process is enabled by default.

Network Management and Monitoring Configuration

1. Network Connectivity Test Configuration
2. Tech-Support Configuration
3. SPAN Configuration
4. sFlow Configuration
5. Configuration for Displaying Device Restart Reasons
6. NTP Configuration
7. SNTP Configuration
8. FTP Server Configuration
9. FTP Client Configuration
10. TFTP Server Configuration
11. TFTP Client Configuration
12. SNMP Configuration
13. RMON Configuration
14. CWMP Configuration
15. SEM Configuration
16. Intelligent Monitoring Configuration
17. NETCONF Configuration

Contents

1 Configuring Network Connectivity Test 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 2
1.2 Restrictions and Guidelines 2
1.3 Configuration Task Summary 2
1.4 Configuring a Ping Connectivity Test 3
1.4.1 Overview 3
1.4.2 Procedure 3
1.5 Configuring a Traceroute Connectivity Test 3
1.5.1 Overview 3
1.5.2 Procedure 3
1.6 Monitoring 4
1.7 Configuration Examples 4
1.7.1 Configuring a Ping Connectivity Test 4
1.7.2 Configuring a Traceroute Connectivity Test 6

1 Configuring Network Connectivity Test

1.1 Introduction

1.1.1 Overview

The network connectivity test tool is used to check whether the network can be connected, and accurately find out the cause of the network failure. Common network communication test tools include packet Internet groper (Ping) and Traceroute. On a network device, the commands corresponding to these two tools are **ping** and **traceroute**.

- The Ping tool is often used to check the network connectivity between devices and the network delay. A larger delay indicates a slower network speed.
- The Traceroute tool helps users learn the topology of the physical and logical connections of the network and efficiency of data transmission.

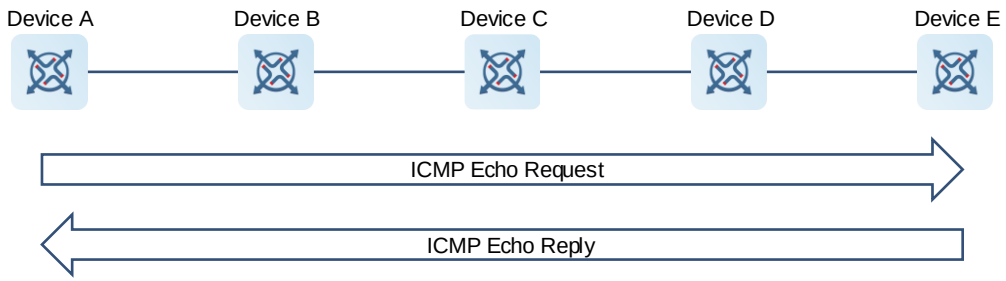
1.1.2 Principles

1. Testing connectivity with Ping

The Ping tool sends an Internet Control Message Protocol (ICMP) Echo Request packet to the destination IP address, requesting the peer to return an ICMP Echo Reply packet to determine whether the two network devices are connected and what is the delay.

The sequence number of the ICMP Echo Request starts from 0. Each time an ICMP Echo Request is sent by the Ping tool, the sequence number increases by 1. The sender sends five ICMP Echo Request packets by default. You can also specify the number of sent ICMP Echo Request packets in the command. If two devices are connected, the receiver returns the same number of ICMP Echo Reply packets.

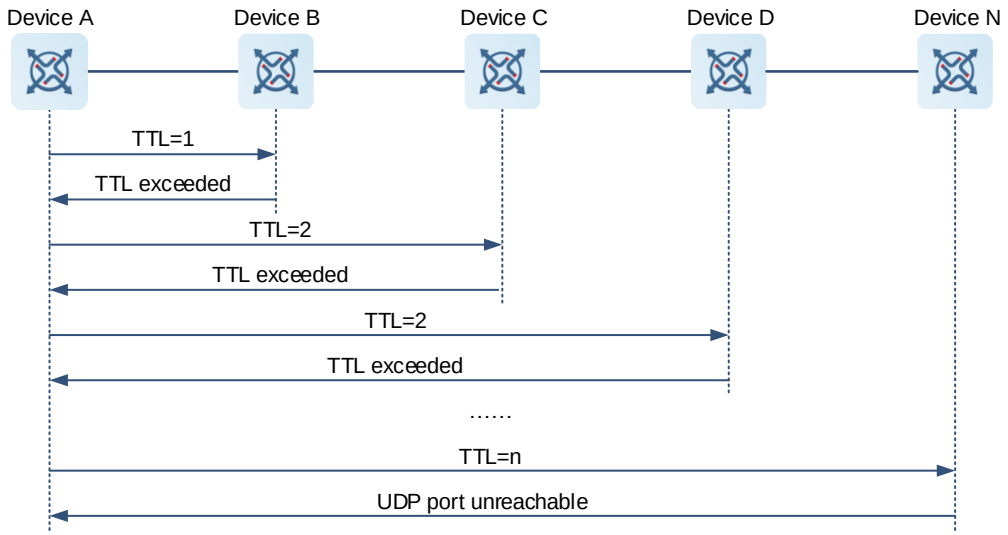
Figure 1-1 Testing Connectivity with Ping



2. Testing connectivity with Traceroute

The Traceroute tool uses the Time To Live (TTL) field in the header of ICMP and IP packets to complete the connectivity check. The process is as follows:

Figure 1-2 Testing Connectivity with Traceroute



(1) Device A sends an ICMP Request packet with the TTL set to 1 through the Traceroute tool. The UDP port number in the packet is an invalid destination port number (greater than 3000).

(2) When the first device, device B, on the path receives this packet, device B decreases the TTL by 1. Then, the TTL changes to 0, and the device discards the packet and returns an ICMP Time Exceeded message.

(3) When Traceroute on device A receives this message, it learns that device B exists on the path and therefore sends a packet with the TTL set to 2 to detect the second device, device C.

(4) Each time when device A sends a packet, Traceroute on device A increases the TTL by 1 to detect another device. This operation repeats until a packet arrives at the destination host. When the packet arrives at the destination host, the host returns an ICMP Port Unreachable message, instead of an ICMP Time Exceeded message. Finally, Traceroute stops the detection and displays the path from the network device to the destination host.

1.1.3 Protocols and Standards

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

1.2 Restrictions and Guidelines

An IP address must be configured for the network device where the Ping and Traceroute operations are executed.

1.3 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Ping Connectivity Test
- Configuring a Traceroute Connectivity Test

1.4 Configuring a Ping Connectivity Test

1.4.1 Overview

You can use Ping connectivity test to check whether a network device is connected to the destination host and whether packets can be transmitted between these two devices.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Check whether the IP address is reachable.

(IPv4 network)

ping [**ip** | **vrf** *vrf-name*] { *hostname* | *ipv4-address* } [**data** *data* | **detail** | **df-bit** | **interval** *interval* | **length** *length* | **ntimes** *times* | **out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | [**source** *interface-type interface-number* | **source** *source-ipv4-address*] | **timeout** *time* | **validate**] *

(IPv6 network)

ping [**ipv6** | **vrf** *vrf-name*] { *hostname* | ipv6-*address* } [**data** *data* | **detail** | **interval** *interval* | **length** *length* | **ntimes** *times* | **out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | [**source** *interface-type interface-number* | **source** *source-ipv6-address*] | **timeout** *time*] *

By default, five 100-byte packets are sent to the specified IP address within two seconds.

1.5 Configuring a Traceroute Connectivity Test

1.5.1 Overview

You can use Traceroute connectivity test on a network device to learn the routing topology and the number of gateways between this device and the destination host.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure an IP packet for tracing.

(IPv4 network)

traceroute [**ip** | **vrf** *vrf-name*] { *hostname* | ipv4-*address* } [**out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | **probe** *probe* | [**source** *interface-type interface-number* | **source** *source-ipv4-address*] | **timeout** *time* | **ttl** *minimum maximum*] *

(IPv6 network)

traceroute [**ipv6** | **vrf** *vrf-name*] { *hostname* | ipv6-*address* } [**out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | **probe** *probe* | [**source** *interface-type interface-number* | **source** *source-ipv6-address*] | **timeout** *time* | **ttl** *minimum maximum*] *

1.6 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

Running the **clear** commands may loss vital information and thus interrupt services.

Table 1-1 Monitoring

Command	Purpose
clear rping table { **all** | **ping-object** *owner-index test-index* | **trace-object** *owner-index test-index* }	Clears the Rping table entries.
show rping detail	Displays detailed information of Rping table entries.

1.7 Configuration Examples

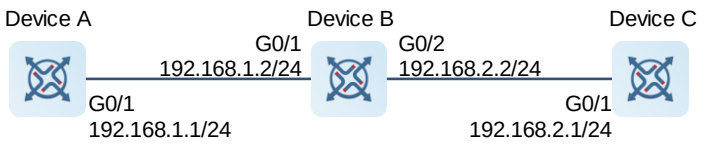
1.7.1 Configuring a Ping Connectivity Test

1. Requirements

Devices A, B, and C are connected to an IP network. It is required to check whether devices A and C can communicate with each other.

2. Topology

Figure 1-3 Testing Connectivity with Ping



3. Notes

- Run the following command in privileged mode: **ping** 192.168.2.1.
- Run the following command in privileged mode: **ping** 192.168.2.1, and specify the length of the sent packet, number of sent packets, and TTL.

4. Procedure

- Use the common Ping function on device A.

  Display the brief Ping result.

```
DeviceA# ping 192.168.2.1
Sending 5, 100-byte ICMP Echoes to 192.168.2.1, timeout is 2 seconds:
```

```
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Display the detailed Ping result.

```
DeviceA# ping 192.168.2.1 detail
Sending 5, 100-byte ICMP Echoes to 192.168.2.1, timeout is 2 seconds:
  < press Ctrl+C to break >
Reply from 192.168.2.1: bytes=100 time=4ms TTL=64
Reply from 192.168.2.1: bytes=100 time=3ms TTL=64
Reply from 192.168.2.1: bytes=100 time=1ms TTL=64
Reply from 192.168.2.1: bytes=100 time=1ms TTL=64
Reply from 192.168.2.1: bytes=100 time=1ms TTL=64

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.
```

- Use the extended Ping function on device A.

Display the brief Ping result.

```
DeviceA# ping 192.168.2.1 length 1500 ntimes 100 data ffff source 192.168.1.1
timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.2.1, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

Display the detailed Ping result.

```
DeviceA# ping 192.168.2.1 length 1500 ntimes 10 data ffff source 192.168.1.1 timeout
3 detail
Sending 20, 1500-byte ICMP Echoes to 192.168.2.1, timeout is 3 seconds:
  < press Ctrl+C to break >
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=2ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64

Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/3 ms.
```

5. Verification

Common Ping function: By default, five 100-byte packets are sent to the specified IP address. Within the specified time (2 seconds by default), the detection information is displayed, and statistical information is output.

Extended Ping function: By default, ten 1500-byte packets are sent to the specified IP address. If there is a response within the specified time (3 seconds), the detection information is displayed, and statistical information is output.

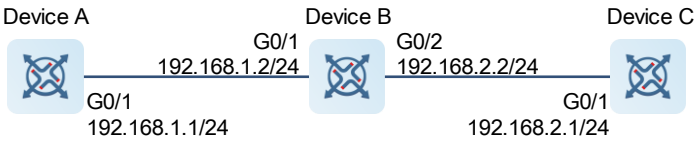
1.7.2 Configuring a Traceroute Connectivity Test

1. Requirements

Devices A, B, and C are connected to an IP network. Device A fails to communicate with device C. It is required to check whether the route between devices A and C is reachable. If the route is unreachable, confirm the faulty network node.

2. Topology

Figure 1-4 Testing connectivity with Traceroute



3. Notes

Run the following command in privileged mode: **traceroute** 192.168.2.1.

4. Procedure

(1) Configure an IP address on devices A, B, and C, respectively. (omitted)

(2) Configure a static route on device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA (config)# ip route 0.0.0.0 0.0.0.0 192.168.1.2
DeviceA (config)# exit
```

(3) Check whether the route between devices A and C is reachable.

```
DeviceA# ping 192.168.2.1
Sending 5, 100-byte ICMP Echoes to 192.168.2.1, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

(4) Check the faulty network node.

```
DEVICEA# traceroute ip 192.168.2.1
  < press Ctrl+C to break >
Tracing the route to 192.168.2.1
1     192.168.1.2        1 msec  1 msec  1 msec
2     *        *        *
3     *        *        *
4     *        *        *
```

5. Verification

The displayed result indicates that the route between devices A and C is unreachable. The packet sent from device A to device C has arrived at device B, but a fault occurs to the connection between devices B and C.

Contents

1 Configuring Tech-Support 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Enabling the Tech-Support Function 1

1.2.1 Overview 1

1.2.2 Restrictions and Guidelines 2

1.2.3 Procedure 3

1.3 Monitoring 3

1 Configuring Tech-Support

1.1 Introduction

1.1.1 Overview

Tech-Support is an information collection function that provides diversified information collection triggering modes according to requirements of the administrator, and collects information on faulty equipment in different modes.

1.1.2 Principles

1. Basic collection

In basic collection mode, the directory files registered by the log framework are collected, including configuration files, Syslog, and CLI operations.

2. Full collection

In full collection mode, the following fault information is collected:

- All fault log files
- Coredump files
- Service realtime fault information

3. Hotkey collection

When the console fails, you can use the hotkey @@@@f to trigger one-click collection. For details about the collected content, see Full collection.

4. Reset key collection

Press the Reset key on the panel for less than 5s to collect the fault information. Five minutes later, the device is reset. For details about the collected content, see Full collection.

5. Storage of the collected content

The collected fault information is stored in the descending order of USB flash drive, **Flash:/**, and **Tmp:/**.

If the collected fault information is not stored on the USB flash drive, at most two compressed packages are stored.

6. Collection of real-time diagnostic information

When a fault occurs, you can run the **show system diag-info** command and necessary CLI commands in debug support mode to collect the related fault information and save it in **diag-info.txt** on the Flash.

1.2 Enabling the Tech-Support Function

1.2.1 Overview

You can use the Tech-Support function to collect detailed fault information of a device and use it for fault location.

1.2.2 Restrictions and Guidelines

- When the device is connected to the console port, you can also use the hotkey **@@@@f** to collect detailed fault information of the device. The @@@@f hotkey operation is often performed when the console crashes. The fault information is packaged in a way similar to the **tech-support package** command.
- Before enabling the Tech-Support function, you are advised to check whether the device has sufficient space to store the fault information.
- To avoid an information collection failure due to insufficient storage space, you are advised to insert the USB flash drive into the device before enabling Tech-Support to avoid information loss. You can use the TFTP function to transfer the compressed packages of the final fault information to a PC.
- If the collected files are too large, it takes a long time to collect the information and services may be affected. To prevent this problem, if the collected coredump files exceed 200 MB or the number of files is too large, a collection failure notification will be displayed. In this case, you need to use other commands to collect coredump files separately.
- The specific procedure is as follows:

  a Run the **show coredump files** command to display the coredump file names.

```
Ruijie# show coredump files
Directory of /xxx/xxx/xxx/ :
 core-xxx-xxx
```

  b Enter the debug support mode, run the **execute diagnose-cmd copy** command to copy the coredump files to the **data** directory, and upload the files to the specified TFTP server.

```
Ruijie# debug support
Ruijie(support)# execute diagnose-cmd copy xxx/xxx/xxx/core-xxx-xxx /data
This operation will modify file? [Y/N]:y
Ruijie(support)# exit
Ruijie# copy flash:/ xxx/xxx/xxx/core-xxx-xxx tftp://xxx.xxx.xxx.xxx/
This operation may overwrite file[tftp:// xxx.xxx.xxx.xxx /core-xxx-xxx]? [Y/N]:y
Press Ctrl+C to quit
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy success.
```

- The compressed packages of fault information are stored as follows:
  - USB flash drive

    If a USB flash drive is inserted into the device, the compressed packages are stored in the root directory of the USB flash drive. You can run the **dir usb0:** command to view these compressed packages.
  - Flash directory

    If no USB flash drive is inserted into the device, the compressed packages are preferentially stored in the Flash directory. You can run the **dir flash:** command to view these compressed packages.
  - **Tmp** directory (memory)

    If no USB flash drive is inserted into the device and the Flash has insufficient space, the compressed packages are stored in the **Tmp** directory. You can run the **dir tmp:** command to view these compressed packages.
- To prevent excessive consumption of space on the storage media after the fault information is collected for

multiple times, a maximum of three compressed packages of fault information can be stored on the same storage medium.

1.2.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(1) Enter the debug configuration mode.

debug support

(2) Enable the Tech-Support function. The configuration tasks below are mutually exclusive. Please configure only one task.

- Run the following command to enable the Tech-Support function:

tech-support package [*component-name* | **basic**]

- Use the hotkey to enable the Tech-Support function.

@@@@f

This command takes effect only when the device is connected to the console port, and is invalid for remote connections, for example, Telnet or SSH connection.

(3) Run the diagnose command:

execute diagnose-cmd { [**device** *device-id*] [**slot all** | **slot** *slot-id* }] [**chip** *chip-id*] *shell-command* | **help** }

1.3 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show system diag-info	Displays the diagnostic information when a fault occurs.

Contents

1 Configuring SPAN 1
1.1 Overview 1
1.1.1 Basic Concepts 1
1.1.2 Working Process 2
1.2 Restrictions and Guidelines 4
1.3 Configuration Task Summary 5
1.4 Configuring SPAN 5
1.4.1 Overview 5
1.4.2 Restrictions and Guidelines 5
1.4.3 Procedure 6
1.5 Configuring RSPAN 6
1.5.1 Overview 6
1.5.2 Restrictions and Guidelines 7
1.5.3 Procedure 7
1.6 Configuring ERSPAN 8
1.6.1 Configuration Tasks 8
1.6.2 Configuring Basic Functions of ERPSAN 8
1.6.3 Configuring Stream-based ERSPAN 9
1.6.4 Configuring ERSPAN Attributes 9
1.7 Monitoring 10
1.8 Configuration Examples 10
1.8.1 Configuring SPAN 10

1.8.2 Configuring RSPAN to Realize One-to-Many SPAN 13

1.8.3 Configuring Basic Functions of ERPSAN 17

1 Configuring SPAN

1.1 Overview

Switch port analyzer (SPAN) is a function that copies packets of a specified port to another port that is connected to a network monitoring device, so as to achieve network monitoring and troubleshooting.

1.1.1 Basic Concepts

1. Session

A session must contain a source port and an output port.

2. Source Port

A source port is also called a monitored port. In a SPAN session, data streams of the source port are monitored for network analysis and troubleshooting.

3. Destination Port

A destination port is also called a monitoring port, and used to receive packets from the source port in a SPAN session.

4. Source Device

A source device is a role in remote SPAN (RSPAN) where the source port resides. It copies packets of the source port and outputs them through the output port of the source device to an intermediate device or the destination device.

5. Reflector Port

A reflector port can be used for "one-to-many RSPAN" (mirroring packets from one port to multiple destination ports). Packets entering a device from the SPAN source port are output from the output port through "reflection" of the reflector port.

6. Destination Device

A destination device is a role in RSPAN where the destination port resides. It forwards the mirrored packets received from the intermediate or source device to the monitoring device through the SPAN destination port.

7. Output Port

An output port on the source device is used to send mirrored packets to a port on an intermediate device or a destination device.

8. SPAN Data Streams

A SPAN session covers data streams in three directions:

- Input data streams

  All packets received by a source port are copied to the destination port. Users can monitor input packets of one or more source ports in a SPAN session.

- Output data streams

All packets transmitted by a source port are copied to the destination port. Users can monitor output packets of one or more source ports in a SPAN session.

- Bidirectional data streams

  Bidirectional data streams include input data streams and output data streams. In a SPAN session, users can monitor data streams of one or more source ports in the input and output directions.

1.1.2 Working Process

SPAN is divided into SPAN, RSPAN, and encapsulated remote switch port analyzer (ERSPAN), depending on whether the source port and destination port of a SPAN session reside on the same device.

1. SPAN Working Process

SPAN is also called local SPAN. In SPAN, the source port and destination port of the same SPAN session must reside on the same device. SPAN can be used to monitor data streams that pass through a device. It copies frames from a port to another port that is connected to a network analyzer to analyze the communication of the port. As shown in Figure 1-1, all packets on port 1 are copied to port 10, and the network analyzer connected to port 10 receives all packets that pass through port 1. The specific process is as follows:

(1) The device identifies and marks the incoming and outgoing packets of the source port.

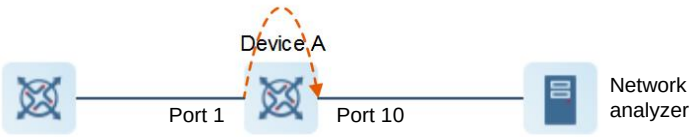
(2) The device searches for the SPAN session to which the monitored port belongs.

(3) The device searches for the destination port corresponding to the SPAN session.

(4) The device copies packets and sends them to the destination port.

(5) The destination port sends the copied packets to the analyzer.

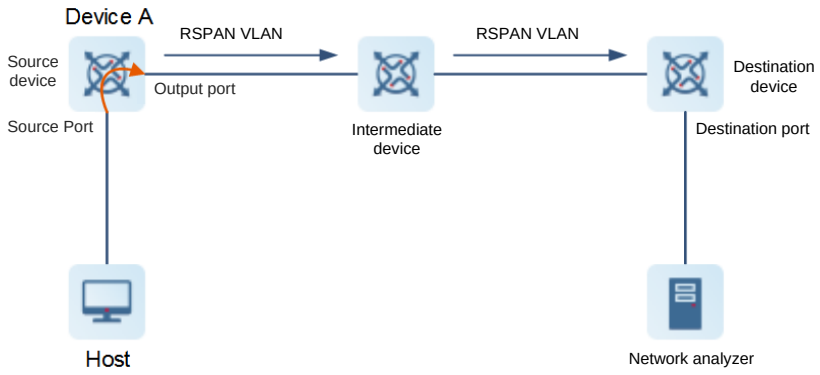
Figure 1-1 SPAN Principles



2. RSPAN Working Process

RSPAN is an extension of SPAN. It breaks the limitation that the source port and destination port of the same SPAN session must reside on the same device, and allows the source port and the destination port to span multiple network devices. A remote VLAN is created for the source device, intermediate device, and destination device, and all ports involved in an RSPAN session must be added to the remote VLAN. Mirrored packets are broadcast in the remote VLAN so that they are transmitted from the source port of the source device to the destination port of the destination device. Figure 1-2 shows the specific working process.

Figure 1-2 RSPAN Principles



(1) Source device

A source device is where the RSPAN source port resides. It copies packets of the source port, and outputs them through the output port of the source device. These packets are forwarded through the remote VLAN to an intermediate device or the destination device.

(2) Intermediate device

An intermediate device resides between the source device and the destination device. It forwards the mirrored packets through the remote VLAN to a next intermediate device or the destination device.

Note

If the source device is directly connected to the destination device, there is no intermediate device.

(3) Destination device

A destination device is where the RSPAN destination port resides. It forwards the mirrored packets received from the remote VLAN to the monitoring device through the RSPAN destination port.

3. ERSPAN Working Process

ERSPAN is an extension of RSPAN. RSPAN packets can be transmitted only at Layer 2 and cannot pass through routing networks. However, ERSPAN can encapsulate the mirrored packets to IP packets through the GRE tunnel and route them to the destination port of the RSPAN device, thus transmitting mirrored packets between routing networks.

Figure 1-3 shows how to forward ERSPAN packets.

(1) The source device copies and encapsulates the incoming packets of the source port.

- Encapsulate the source and destination IP addresses of the GRE packet.
- Set the TTL and DSCP of the GRE packet.

Figure 1-4 shows the header format of a packet encapsulated in ERSPAN.

(2) The source port forwards mirrored packets to the destination device through the GRE tunnel.

(3) The destination device decapsulates GRE packets to remove the header encapsulated by ERSPAN, and forwards the packets to the destination port.

(4) The destination port forwards the mirrored packets to the data analyzer.

Caution

The IP packets after GRE encapsulation can be normally routed to the destination device in the network. Therefore, the destination IP address is generally the next-hop IP address of the route. That is, the output port of the source device is the next-hop egress of the L3 path where the destination IP address to be encapsulated is located. The output port must be reachable, and can be an SVI, an L3AP, or a routed port.

Figure 1-3 ERSPAN Principles

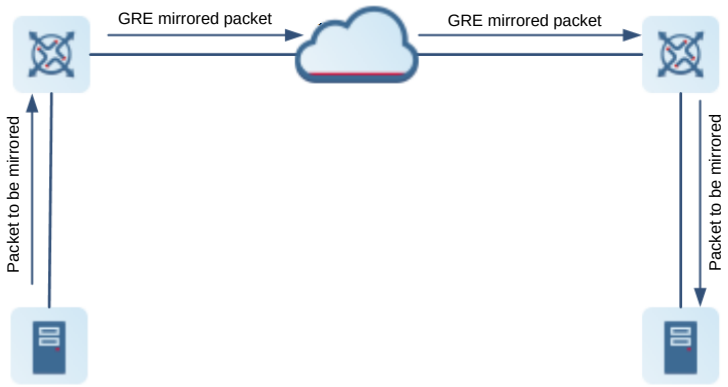


Figure 1-4 Format of an Encapsulated Packet in ERSPAN

MAC_HEADER(14/18B)	IP_HEADER(20B)	GRE_HEADER(48B)	L2_Mirrored_Packet(untagged)

4. Stream Mirroring Principles

Stream mirroring is to associate the source port with an ACL on the basis of SPAN, and filter packets based on the ACL rules, so as to mirror only specified packets. Only the packets matching the permit ACE in the ACL on the source port can be mirrored to the destination port. A source port can be associated with only one ACL. Currently, the standard ACL, extended ACL, MAC ACL, and custom ACL can be associated.

ACL-based SPAN is supported only in the receive (RX) direction, but not in the transmit (TX) direction.

1.2 Restrictions and Guidelines

- A source port has the following features:
  - The source port can be an L2 port, L3 port, or aggregation port.
  - Data streams on multiple source ports on the source device can be mirrored to a specified output port.
  - The source port and the output port cannot be the same one.
  - When the source port is an L3 port, L2 and L3 packets can be monitored.
  - Upon bidirectional monitoring of multiple ports, a packet is received from one port and output from another port, and monitoring is effective as long as one packet is monitored among these ports.
  - When a port is STP enabled and in the block state, the incoming and outgoing packets of the port can

also be monitored.

- The source port and the destination port can belong to the same VLAN or different VLANs.

- A destination port has the following features:
  - The destination port can be a switched port, a routed port, or an aggregation port.
  - A destination port cannot be used as a source port simultaneously.
  - The SPAN destination port is used for the Spanning Tree Protocol (STP) calculation.
- A configured session ID cannot be used as the ID of another SPAN session.
- If a source port is added to an aggregation port, the source port exits the SPAN session.

  By default, the switch function is disabled on the SPAN destination port, and the destination port only receives mirrored packets and does not forward data. If the destination port needs to forward data, the switch function must be enabled; otherwise, packets passing through this port will be discarded.
- Due to other reasons (such as port security), incoming packets of a source port may be discarded, but it does not affect the SPAN function, and these packets are still mirrored to the destination port. Due to other reasons, packets sent from other ports to a source port may be discarded, and these packets are not sent to the destination port.
- If the format of a packet output from the source port is changed, for example, the source MAC, destination MAC, VLAN ID, and TTL of the packet change, the format of the packet mirrored to the destination port will change as well.
- You can configure the following types of ACL on the source port to filter mirrored packets: standard ACL, extended ACL, MAC ACL, and custom ACL.

1.3 Configuration Task Summary

SPAN configuration includes the following tasks:

- Configuring SPAN
- Configuring RSPAN
- Configuring ERSPAN
  - a Configuring Basic Functions of ERPSAN
  - b (Optional) Configuring Stream-based ERSPAN
  - c (Optional) Configuring ERSPAN Attributes

1.4 Configuring SPAN

1.4.1 Overview

SPAN copies packets of the designated port or designated VLAN to the port connected to the data monitoring device, so that you can use the data monitoring device to analyze these copied packets for network monitoring and troubleshooting.

1.4.2 Restrictions and Guidelines

- When configuring the SPAN source port, you can specify the following items as the data source simultaneously: some VLANs, an interface, and specified streams on the specified port.

- When configuring the SPAN source port, if you specify a VLAN as the data source, you cannot specify an interface or streams on the specified port as the data source.
- When configuring the SPAN source port, if you specify some VLANs as the data source, you must also specify the source port.
- If you change the VLAN configuration on the source port, the configuration takes effect immediately.
- If you change the VLAN configuration on the destination port, the configuration takes effect immediately.
- If you disable the source or destination port, the SPAN function does not take effect.
- If you configure a VLAN or a VLAN list as the SPAN source, ensure that the destination port has sufficient bandwidth for receiving mirrored data of the entire VLAN (or VLAN list).
- If you add or delete a VLAN source port to or from an effective SPAN session, you need to re-apply the entire SPAN session. Therefore, a few existing mirrored packets may be lost.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a SPAN source port. Configure at least one of the following tasks.

- Specify an interface as the data source of SPAN.

  monitor session *session-number* **source interface** *interface-type interface-number* [**both** | **rx** | **tx**]

- Specify some streams of an interface as the data source of SPAN.

  monitor session *session-number* **source interface** *interface-type interface-number* **rx acl** { *acl-name* | *acl-number* }

- Exclude one or more VLANs as the data source of SPAN.

  monitor session *session-num* **filter vlan** *vlan-id-list* **rx**

  This command must be configured together with monitor session source **interface** or monitor session source **interface acl**

- Specify one or more VLANs as the data source of SPAN.

  monitor session *session-num* **source vlan** *vlan-id-list* **rx**

  This configuration is mutually exclusive with the preceding three configurations.

By default, no source port is configured for a SPAN session.

(4) Configure a SPAN destination port.

monitor session *session-num* **destination interface** *interface-type interface-number* [**switch**]

By default, no SPAN destination port is configured.

1.5 Configuring RSPAN

1.5.1 Overview

- Configure a source port and destination port on the source device of an RSPAN session and configure the

destination port on the destination device.

- Configure the destination port on the RSPAN destination device to monitor any packets that are transmitted or received by the source port.

1.5.2 Restrictions and Guidelines

- All ports involved in RSPAN must be added to a remote VLAN.
- A remote VLAN must be configured on each device, their VLAN IDs must be consistent, and all ports that participate in a session must be added to the VLAN. It is not recommended that common ports be added to a remote VLAN.
- Do not configure a port that is connected to an intermediate device or a destination device as an RSPAN source port. Otherwise, traffic on the network may be in chaos.
- The reflector port cannot serve as a normal port to forward packets. You are advised to configure a port in Down state as the reflector port, and not to add other configurations for this port.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VLAN configuration mode.

vlan *vlan-id*

(4) Configure a remote VLAN.

remote-span

By default, no remote VLAN is configured.

(5) Exit the VLAN configuration mode.

exit

(6) Configure an RSPAN source device.

monitor session *session-num* **remote-source**

By default, no source device is configured for an RSPAN session.

(7) (Optional) Configure the MAC loopback function on the source device.

a Enter the interface configuration mode.

interface *interface-type interface-number*

b Enable the MAC loopback function of the interface.

mac-loopback

By default, MAC loopback is disabled for an interface.

(8) Configure a source port on the source device. Configure at least one of the following tasks.

- Specify an interface as the data source of ERSPAN.

  monitor session *session-number* **source interface** *interface-type interface-number* [**both** | **rx** | **tx**]

- Specify streams of an interface as the data source of RSPAN.

monitor session *session-number* **source interface** *interface-type interface-number* **rx acl** { *acl-name* | *acl-number* }

By default, no source port on the source device is configured for an RSPAN session.

(9) Configure an RSPAN destination device.

monitor session *session-num* **remote-destination**

By default, no destination device is configured for an RSPAN session.

(10) Configure an output port on the source device or a destination port on the destination device.

monitor session *session-number* **destination remote vlan** *remote-vlan-id* **interface** *interface-type interface-number* [**switch**]

By default, no output port on the RSPAN source device or no destination port on the RSPAN destination device is configured.

1.6 Configuring ERSPAN

1.6.1 Configuration Tasks

ERSPAN configuration includes the following tasks:

(1) Configuring Basic Functions of ERPSAN

(2) (Optional) Configuring Stream-based ERSPAN

(3) (Optional) Configuring ERSPAN Attributes

1.6.2 Configuring Basic Functions of ERPSAN

1. Overview

After ERSPAN is configured, a network analyzer can be used to monitor users. Devices can normally exchange data with each other.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ERSPAN session.

monitor session *session-number* **erspan-source**

No ERSPAN session is configured by default.

(4) Specify an interface as the data source of ERSPAN.

source interface *interface-type interface-number* { [**rx** | **tx** | **both**] }

By default, no source port is configured. If a source port is configured, the mirroring direction is **both** by default.

When a sub-interface is configured as the source port, mirroring is supported only in the inbound direction.

(5) Configure the source IP address for encapsulation.

original ip address *ipv4-address*

By default, no source IP address is configured for GRE encapsulation.

(6) Configure the destination IP address for encapsulation.

destination ip address *ipv4-address*

By default, no encapsulation type or destination IP address is configured.

1.6.3 Configuring Stream-based ERSPAN

1. Overview

After stream-based ERSPAN is configured, a network analyzer can be used to monitor specified packets. Devices can normally exchange data with each other

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ERSPAN session.

monitor session *session-number* **erspan-source**

(4) (Optional) Specify data streams of an interface as the data source of ERSPAN.

source interface *interface-type interface-number* **rx acl** { *acl-name* | *acl-number* }

By default, no source port is configured. If a source port is configured, the mirroring direction is **both** by default.

(5) Configure the source IP address for encapsulation.

original ip address *ip-address*

(6) Configure the destination IP address for encapsulation.

destination ip address *ip-address*

1.6.4 Configuring ERSPAN Attributes

1. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ERSPAN session.

monitor session *session-number* **erspan-source**

(4) Configure attributes of an ERSPAN session. The following configurations are optional. Select at least one of the configurations as actually needed.

(5) (Optional) Configure the TTL of the encapsulated IP packet.

ip ttl *ttl-value*

The default TTL of the encapsulated IP packet is **64**.

(6) (Optional) Configure the DSCP of the encapsulated IP packet.

ip dscp *dscp-value*

The default DSCP of the encapsulated IP packet is **0**.

(7) (Optional) Associate ERSPAN with a VRF.

vrf *vrf-name*

By default, no VRF is associated with ERSPAN.

When this function is configured, the VRF must be already configured.

(8) (Optional) Shut down the ERSPAN session.

shutdown

The session is enabled by default.

1.7 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Table 1-1 Monitoring

Command	Purpose
show monitor [**session** *session-number*]	Displays the SPAN session information.
debug span	Debugs the SPAN.

1.8 Configuration Examples

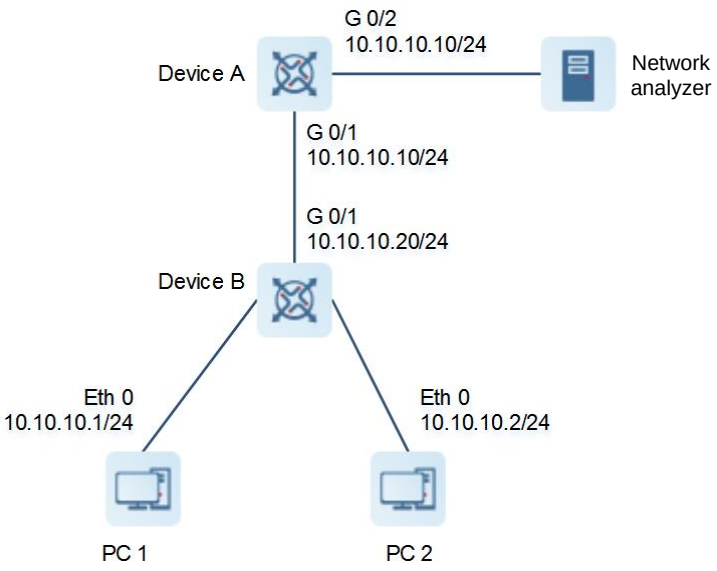
1.8.1 Configuring SPAN

1. Requirements

As shown in Figure 1-5, after appropriate configuration, the network analyzer can monitor all data streams forwarded by device A to device B and specified data streams of device B (for example, data streams from PC 1 and PC 2).

2. Topology

Figure 1-5 SPAN Topology



3. Notes

- Add GigabitEthernet 0/1 and GigabitEthernet 0/2 of device A to VLAN 1. Create SVI 1 and set the address of SVI 1 to 10.10.10.10/24.
- Add GigabitEthernet 0/1 of device B to VLAN 1. Create SVI 1 and set the address of SVI 1 to 10.10.10.20/24.
- Set the IP addresses of PC 1 and PC 2 to 10.10.10.1/24 and 10.10.10.2/24, respectively.
- Configure SPAN for Device A and configure ports GigabitEthernet 0/1 and GigabitEthernet 0/2 as the source port and destination port of SPAN respectively. Monitor all data streams forwarded by device A to device B and specified data streams of device B.

4. Procedure

Add GigabitEthernet 0/1 and GigabitEthernet 0/2 of device A to VLAN 1.

```
DeviceA> enable
DeviceA# configure
DeviceA(config)# vlan 1
DeviceA(config-vlan)# exit
```

On device A, create SVI 1 and set the address of SVI 1 to 10.10.10.10/24.

```
DeviceA(config)# interface VLAN 1
DeviceA(config-if-VLAN 1)# ip address 10.10.10.10 255.255.255.0
DeviceA(config-if-VLAN 1)# exit
```

Add GigabitEthernet 0/1 of device B to VLAN 1.

```
DeviceB# configure
DeviceB(config)# vlan 1
DeviceB(config-vlan)# exit
```

On device B, create SVI 1 and set the address of SVI 1 to 10.10.10.20/24.

```
DeviceB (config)# interface VLAN 1
DeviceB(config-if-VLAN 1)# ip address 10.10.10.20 255.255.255.0
DeviceB(config-if-VLAN 1)# exit
```

On device A, configure an ACL to match packets with the source address 10.10.10.20.

```
DeviceA(config)# access-list 100 permit ip host 10.10.10.20 any
```

On device A, configure GigabitEthernet 0/1 as the SPAN source port, and monitor all data streams forwarded by device A to device B and specified data streams of device B.

```
DeviceA(config)# monitor session 1 source interface gigabitEthernet 0/1 tx
DeviceA(config)# monitor session 1 source interface gigabitEthernet 0/1 rx acl 100
```

On device A, configure GigabitEthernet 0/2 on device A as the SPAN destination port.

```
DeviceA(config)# monitor session 1 destination interface gigabitEthernet 0/2
```

5. Verification

Run the **show monitor** command to check whether the SPAN configuration is correct.

```
DeviceA# show monitor
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
  GigabitEthernet 0/1        frame-type TX Only
src-intf:
  GigabitEthernet 0/1        frame-type RX Only
rx acl id 100
dest-intf:
  GigabitEthernet 0/2
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip access-list extended 100
 10 permit ip host 10.10.10.20 any
!
interface VLAN 1
 ip address 10.10.10.10 255.255.255.0
!
monitor session 1 destination interface GigabitEthernet 0/2
monitor session 1 source interface GigabitEthernet 0/1 tx
monitor session 1 source interface GigabitEthernet 0/1 rx acl 100
!
end
```

- Device B configuration file

```
hostname DeviceB
```

```
!
interface VLAN 1
 ip address 10.10.10.20 255.255.255.0
!
end
```

1.8.2 Configuring RSPAN to Realize One-to-Many SPAN

Caution

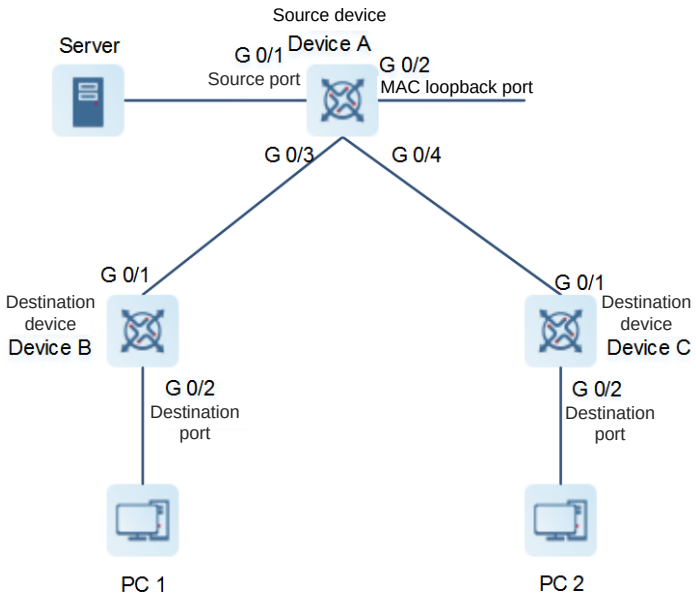
When deploying One-to-Many SPAN, you must run the **switchport trunk allowed vlan remove** *vlan-list* command to remove the flood VLANs from a trunk interface on each SPAN device. Otherwise, the trunk interface may be fully occupied by the traffic flood, causing service interruption.

1. Requirements

As shown in Figure 1-6, the RSPAN function enables the network analyzer to monitor users connected to the source device A from the destination devices B and C. The devices can normally exchange data with each other.

2. Topology

Figure 1-6 Topology of RSPAN Used to Realize One-to-Many SPAN



3. Notes

- Configure device A as the source device. Configure a remote VLAN. Configure GigabitEthernet 0/1 directly connected to users as the source port, GigabitEthernet 0/3 and GigabitEthernet 0/4 connected to the destination device as the output ports, and GigabitEthernet 0/2 as the MAC loopback port to realize the reflection function of one-to-many SPAN. Configure the switching function of the output port.
- Configure devices B and C as the destination devices. Configure a remote VLAN. Configure GigabitEthernet

0/1 connected to the source device as the source port. Configure a trunk port. Configure GigabitEthernet 0/2 connected to the network analyzer as the SPAN destination port, and configure the switching function for the SPAN destination port.

4. Procedure

(1) Configure device A as the source device.

a. Configure a remote VLAN.

```
DeviceA> enable
DeviceA# configure
DeviceA(config)# vlan 7
DeviceA(config-vlan)# remote-span
DeviceA(config-vlan)# exit
```

b. Configure a source port.

```
DeviceA(config)# monitor session 1 remote-source
DeviceA(config)# monitor session 1 source interface GigabitEthernet 0/1 both
```

c. Configure an output port.

```
DeviceA(config)# monitor session 1 destination remote vlan 7 interface
GigabitEthernet 0/2 switch
```

d. Configure a loopback port.

```
DeviceA(config)# interface GigabitEthernet 0/2
DeviceA(config-if)# mac-loopback
DeviceA(config-if)# switchport access vlan 7
DeviceA(config-if)# exit
DeviceA(config)# interface range GigabitEthernet 0/3-4
DeviceA(config-if-range)# switchport mode trunk
```

(2) Configure device B as the destination device.

a. Configure a remote VLAN.

```
DeviceB> enable
DeviceB# configure
DeviceB(config)# vlan 7
DeviceB(config-vlan)# remote-span
DeviceB(config-vlan)# exit
```

b. Configure a destination port.

```
DeviceB(config)# monitor session 1 remote-destination
DeviceB(config)# monitor session 1 destination remote vlan 7 interface
GigabitEthernet 0/2 switch
DeviceB(config)# interface GigabitEthernet 0/1
DeviceB(config-if)# switchport mode trunk
```

(3) Configure device C as the destination device.

a. Configure a remote VLAN.

```
DeviceC> enable
DeviceC# configure
DeviceC(config)# vlan 7
```

```
DeviceC(config-vlan)# remote-span
DeviceC(config-vlan)# exit
```

b. Configure a destination port.

```
DeviceC(config)# monitor session 1 remote-destination
DeviceC(config)# monitor session 1 destination remote vlan 7 interface
GigabitEthernet 0/2 switch
DeviceC(config)# interface GigabitEthernet 0/1
DeviceC(config-if)# switchport mode trunk
```

5. Verification

Run the **show monitor** command on device A to view the SPAN source device configurations.

```
DeviceA# show monitor
sess-num: 1
span-type: SOURCE_SPAN
src-intf:
GigabitEthernet 0/1     frame-type Both
dest-intf:
GigabitEthernet  0/2
Remote vlan 7
mtp_switch on
```

Run the **show monitor** command on devices B and C to view the SPAN destination device configurations. Device B is taken as an example below:

```
DeviceB# show monitor
sess-num: 1
span-type: DEST_SPAN
dest-intf:
GigabitEthernet  0/2
Remote vlan 7
mtp_switch on
```

6. Configuration Files

- Device A configuration file of

```
hostname DeviceA
!
vlan 7
!
 remote-span
!
interface GigabitEthernet 0/2
 mac-loopback
 switchport access vlan 7
!
interface GigabitEthernet 0/3
switchport mode trunk
interface GigabitEthernet 0/4
```

```
switchport mode trunk
!
monitor session 1 remote-source
monitor session 1 source interface GigabitEthernet 0/1 both
monitor session 1 destination remote vlan 7 interface GigabitEthernet0/2 switch
!
end
```

- Device B configuration file

```
hostname DeviceB
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
monitor session 1 remote-destination
monitor session 1 destination remote vlan 7 interface GigabitEthernet0/2 switch
!
end
```

- Device C configuration file

```
hostname Device
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/1
 switchport mode trunk
 !
monitor session 1 remote-destination
monitor session 1 destination remote vlan 7 interface GigabitEthernet 0/2 switch
!
end
```

7. Common Errors

- A remote VLAN must be configured on the source device, intermediate device, and destination device, and their VLAN IDs must be consistent.
- Packet loss may occur if packets of a port with large bandwidth are mirrored to a port with small bandwidth.
- One MAC loopback port and multiple output ports need to be configured to implement one-to-many RSPAN.

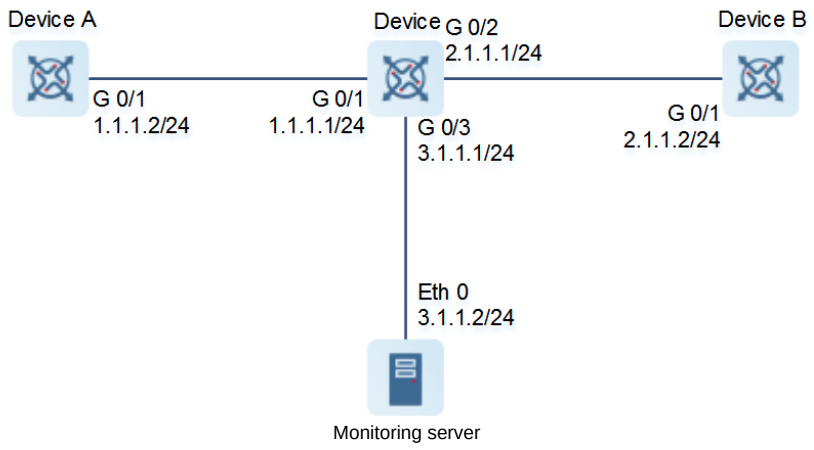
1.8.3 Configuring Basic Functions of ERPSAN

1. Requirements

As shown in Figure 1-7, the network administrator wants to use the network analyzer to monitor traffic on devices A and B. For device A, packets in both directions are monitored. For device B, only some incoming packets are monitored.

2. Topology

Figure 1-7 Topology of ERSPAN



3. Notes

- Configure reachable L3 routes between devices.
- Configure device C as the source device. Configure GigabitEthernet 0/1 and GigabitEthernet 0/2 as the source ports, mirror packets in both directions on GigabitEthernet 0/1, mirror packets with the destination IP address 2.1.1.1 on GigabitEthernet 0/2, and configure GigabitEthernet 0/3 as the output port.

4. Procedure

Configure the IP address of Device.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# ip address 1.1.1.1 255.255.255.0
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# interface gigabitEthernet 0/2
Device(config-if-GigabitEthernet 0/1)# ip address 2.1.1.1 255.255.255.0
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# interface gigabitEthernet 0/3
Device(config-if-GigabitEthernet 0/1)# ip address 13.1.1.1 255.255.255.0
Device(config-if-GigabitEthernet 0/1)# exit
```

Configure the IP address of device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 1.1.1.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Configure the IP address of device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 2.1.1.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure an ACL on Device.

```
Device(config)#access-list 1 permit host 1.1.1.1
```

Create ERSPAN Session 1, and configure Device as the source device. Configure GigabitEthernet 0/1 as the source port, and mirror packets in both directions. Configure GigabitEthernet 0/2 as the source port, and mirror packets with the destination IP address 1.1.1.1.

```
Device(config)# monitor session 1 erspan-source
Device(config-mon-erspan-src)# source interface gigabitEthernet 0/1 both
Device(config-mon-erspan-src)# source interface gigabitEthernet 0/2 rx acl acl1
Device(config-mon-erspan-src)# origin ip address 10.1.1.2
Device(config-mon-erspan-src)# destination ip address 3.1.1.2
```

5. Verification

Check that the L3 route between Device and Device A is reachable.

```
Device# ping 1.1.1.2
Sending 5, 100-byte ICMP Echoes to 1.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/8 ms.
```

Check that the L3 route between Device and Device B is reachable.

```
Device# ping 2.1.1.2
Sending 5, 100-byte ICMP Echoes to 2.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/8 ms.
```

Check that the L3 route between Device and the network analyzer is reachable.

```
Device# ping 3.1.1.2
Sending 5, 100-byte ICMP Echoes to 3.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/8 ms.
```

Run the **show access-lists** command to check that the ACL configuration takes effect.

```
Device# show access-lists
```

```
ip access-list standard 1
 10 permit host 1.1.1.1
```

Run the **show monitor** command to check that the ERSPAN session is in Active state in the configuration result.

```
Device# show monitor
sess-num: 1
span-type: ERSPAN_SOURCE
src-intf:
  GigabitEthernet 0/1        frame-type: Both       TX status: Active   RX status:
Active
src-intf:
  GigabitEthernet 0/2        frame-type: RX Only     Rx acl id: 1
status: Active
original ip address: 2.1.1.2
destination ip address: 3.1.1.2
ip ttl: 64
ip dscp: 0
vrf: default
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 ip address 1.1.1.2 255.255.255.0
!
end
```

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/1
 ip address 2.1.1.2 255.255.255.0
!
end
```

- Device configuration file

```
hostname Device
!
ip access-list standard 1
 10 permit host 1.1.1.1
!
interface GigabitEthernet 0/1
 ip address 1.1.1.1 255.255.255.0
!
```

```
interface GigabitEthernet 0/2
 ip address 2.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/3
 ip address 3.1.1.1 255.255.255.0
!
monitor session 1 erspan-source
 source interface gigabitEthernet 0/1 both
 source interface gigabitEthernet 0/2 rx acl acl1
 origin ip address 10.1.1.2
 destination ip address 3.1.1.2

!
end
```

7. Common Errors

- The session ID used to configure ERSPAN is already configured with RSPAN or LOCAL SPAN.
- The L3 route between the source device and destination device is unreachable.

Contents

1 Configuring sFlow.....1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles.....1

1.1.3 Protocols and Standards 3

1.2 Configuration Task Summary 4

1.3 Configuring sFlow 4

1.3.1 Configuring Basic Functions of sFlow 4

1.3.2 Configuring Optional Parameters of sFlow.....5

1.4 Monitoring 6

1.5 Configuration Examples.....7

1.5.1 Configuring Basic Functions of sFlow 7

1 Configuring sFlow

1.1 Introduction

1.1.1 Overview

Sampled flow (sFlow) is a network monitoring technology based on message sampling. It is mainly used for traffic statistics analysis when the network traffic is huge.

sFlow has the following advantages:

- Accurate: sFlow supports accurate monitoring of traffic on a Gigabit network or a network with higher bandwidth.
- Scalable: One sFlow Collector can monitor thousands of sFlow Agents, and it has high scalability.
- Low cost: sFlow Agent is embedded in a network device, and its cost is low.

1.1.2 Principles

The sFlow system consists of an sFlow Agent embedded in a device and a remote sFlow Collector. The sFlow Agent obtains interface statistics and data from the network device by using specific sampling technologies, encapsulates the information into sFlow packets, and sends them to the sFlow Collector. The sFlow Collector analyzes sFlow packets and displays the analysis results.

- **sFlow Agent**

  An sFlow Agent is embedded in a network device. Generally, one network device serves as an sFlow Agent.

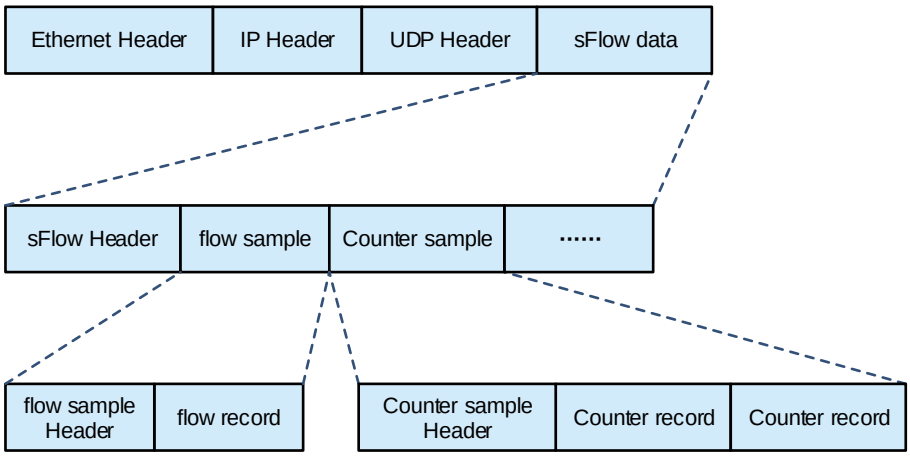
- **sFlow Collector**

  An sFlow Collector can be a PC or server that receives and analyzes sFlow packets from the sFlow Agent. A PC or server installed with the software used for sFlow packet analysis can be regarded as an sFlow Collector.

  The sFlow Agent performs flow sampling and counter sampling, encapsulates sampled data into sFlow packets, and sends them to the sFlow Collector.

  sFlow packets are encapsulated in UDP. Figure 1-1 shows the sFlow packet format.

Figure 1-1 sFlow Packet Format



Note

One sFlow packet may contain one or more flow samples and counter samples.

Figure 1-2 sFlow Header

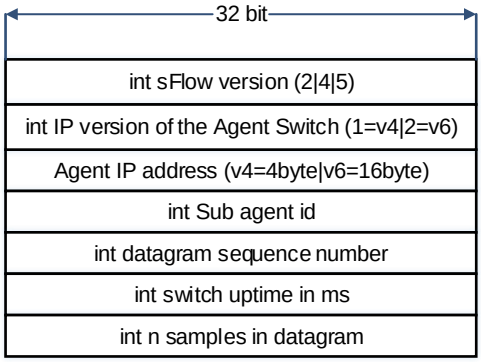


Table 1-1 sFlow Header Description

Field	Description
sFlow version	sFlow version. V2, V4, and V5 are available. Currently, Ruijie supports V5 only.
IP version of the agent/switch	IP address version of the sFlow Agent
Agent IP address	IP address of the sFlow Agent
Sub agent id	Sub agent ID
Datagram sequence number	Serial number of an sFlow packet
Switch uptime	Duration from device startup to the current time

Field	Description
n samples in datagram	Number of samples in an sFlow packet. One sFlow packet contains one or more flow samples and counter samples.

1. Flow sampling

Based on the sampling rate configured for the specified interface, the sFlow Agent device performs flow sampling on packets through this interface, including copying the packet header, extracting the Ethernet header and IP header of each packet, and obtaining the route information of each packet. Then, the sFlow Agent encapsulates the flow sampling result into sFlow packets and sends them to the sFlow Collector for analysis.

Table 1-2 Description of Fields in the Flow Record Part of the sFlow Packet

Field	Description
Raw packet	All or part of the header of the original packet (the extracted length depends on the configuration) is extracted and encapsulated into an sFlow packet and then sent to the Collector.
Extended Switch Data	For an Ethernet packet, the Ethernet header is parsed and encapsulated into an sFlow packet and then sent to the Collector.
Extended VNI Data	VNI ID of a VXLAN packet

2. Counter sampling

In counter sampling, the sFlow Agent periodically obtains the statistics and CPU usage from a specified interface. The sFlow Agent periodically performs interface polling, obtains the statistics from an interface where the counter sampling timer expires, encapsulates the statistics into an sFlow packet, and sends it to the sFlow Collector for analysis.

Table 1-3 Description of Fields in the Counter Sampling Result

Field	Description
Generic Interface Counters	General interface statistics, including basic interface information and general interface traffic statistics
Ethernet Interface Counters	Ethernet-related traffic statistics of an Ethernet interface

1.1.3 Protocols and Standards

- sFlow Version 5: sFlow V5
- RFC 1014: XDR: External Data Representation standard

1.2 Configuration Task Summary

sFlow configuration includes the following tasks:

(1) Configuring Basic Functions of sFlow

(2) (Optional) Configuring Optional Parameters of sFlow

1.3 Configuring sFlow

1.3.1 Configuring Basic Functions of sFlow

1. Overview

- sFlow Agent and sFlow Collector can communicate with each other.
- Traffic flowing through the interface are sampled based on the default sampling rate and sent to the sFlow Collector for analysis.
- Statistics of the interface are periodically sent to the sFlow Collector based on the default sampling interval for analysis.

2. Restrictions and Guidelines

- The forwarding performance of an interface may be affected after flow sampling is enabled.
- To enable the sFlow Collector to analyze the flow sampling results, you must configure the IP address of the sFlow Collector on the sFlow Agent device.
- The sFlow Agent address must be a valid address. That is, the sFlow Agent address cannot be a multicast or broadcast address. It is recommended that the IP address of the sFlow Agent device be used.
- When the **vrf** parameter is configured, the corresponding VRF instance must exist. If you configure a VRF instance for an sFlow Collector address and later remove this VRF instance, the sFlow Collector address will be removed as well.
- You can enable flow sampling on a physical or an aggregation port.
- **sflow enable**
  - This command can be configured on a physical or an aggregation port.
  - If the direction is not specified, flow sampling is enabled in both the inbound and outbound directions.
  - Counter sampling is enabled when flow sampling is enabled in any direction of an interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the sFlow Agent address.

sflow agent { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **interface** [**ipv6**] *interface-type interface-number* }

No sFlow Agent address is configured by default.

(4) Configure the sFlow Collector address.

sflow collector *collector-id* **destination** { *ipv4-address* | **ipv6** *ipv6-address* } *udp-port-number* [**vrf** *vrf-name*] [**description** *collector-description*]

No sFlow Collector address is configured by default.

(5) Configure the ID of the sFlow Collector for flow sampling.

sflow flow collector *collector-id*

No ID of the sFlow Collector is configured for flow sampling by default.

(6) Configure the ID of the sFlow Collector for counter sampling.

sflow counter collector *collector-id*

No ID of the sFlow Collector is configured for counter sampling by default.

(7) Enable the counter sampling and flow sampling functions.

sflow enable [{ **ingress** | **egress** }

The sFlow function is disabled by default.

1.3.2 Configuring Optional Parameters of sFlow

1. Overview

You can adjust the data sampling accuracy by modifying relevant parameter attributes of sFlow.

2. Restrictions and Guidelines

- You can run the **sflow collector** command to configure the payload size of an sFlow packet, excluding the Ethernet header, IP header, and UDP header. One or more flow samples and counter samples can be encapsulated to an sFlow packet. When the maximum sFlow packet size is configured, different numbers of sFlow packets may be output after the same number of flow samples or counter samples are processed. If the maximum size is greater than MTU, the output sFlow packet is segmented.
- The **sflow sampling-rate** command is used to configure the global flow sampling rate. This configuration applies to all interfaces. The flow sampling rate may affect the sFlow sampling accuracy. A lower sampling rate indicates a higher accuracy and a larger CPU consumption, which may affect the forwarding performance of the interface.
- You can run the **sflow flow max-header** command to modify the configuration of packets sent to the sFlow Collector. For example, if you are concerned about the IP header, set the length to 56 bytes. During flow sampling, the first 56 bytes of a sample packet are encapsulated to the sFlow packet.
- This command is used to configure the maximum number of bytes that can be copied from the header of the original packet. The copied content is recorded in the generated sample. The protocol requires byte alignment during packet encapsulation, that is, the actual length of a sent packet is a multiple of 4. Therefore, the length of a collected packet may exceed the configured length. For example, when the maximum length is set to any of 21, 22, 23, and 24, the actual output packet length is 24.
- The **sflow counter interval** command is used to configure the global sFlow counter sampling interval. This configuration applies to all interfaces.
- The **sflow source** command is used to configure the source IP address of output packets. The default source address of output sFlow packets is the local device IP address which is used to ping the destination IP address. If the source interface is specified, the primary address (or the first global IPv6 address if any) of

the interface is the source IP address of output packets. If the source interface is not specified, the default source address is used.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum size of the output sFlow packet.

sflow collector *collector-id* **max-datagram-size** *datagram-size*

By default, the maximum size of the output sFlow packet is **1400**.

(4) Configure the sFlow flow sampling rate.

sflow sampling-rate *sampling-rate*

The default sFlow flow sampling rate is **8192**.

(5) Configure the maximum length of the packet header copied during flow sampling.

sflow flow max-header *sampling-length*

By default, the maximum length of the packet header copied during sFlow flow sampling is **64**.

(6) Configure the sampling interval.

sflow counter interval *sampling-interval-time*

The interface where counter sampling is enabled sends the interface statistics to the sFlow Collector at the sampling interval.

(7) Configure the source address of output sFlow packets.

sflow source { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **interface** [**ipv6**] *interface-type interface-number* }

By default, the source address of output sFlow packets is the local device IP address which is used to ping the destination IP address.

1.4 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-4 sFlow monitoring

Command	Purpose
show sflow	Displays the sFlow configuration.
show sflow capacity	Display the sFlow capacity supported by the device.

1.5 Configuration Examples

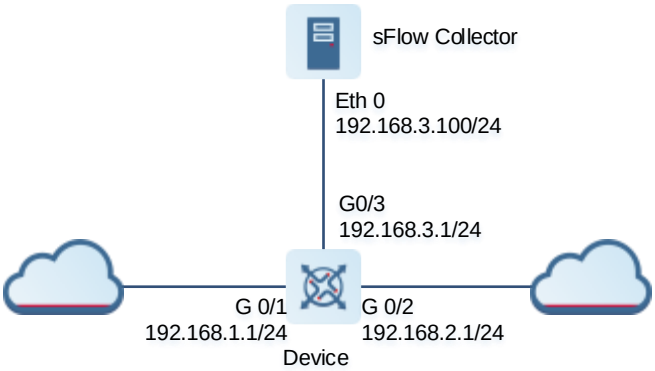
1.5.1 Configuring Basic Functions of sFlow

1. Requirements

Start the device that serves as the sFlow Agent, enable flow sampling and counter sampling on port G 0/1, monitor the traffic in the 192.168.1.0 network segment, encapsulate the sampling result into sFlow packets at regular intervals or when the buffer is full, and send these packets to the sFlow Collector for traffic analysis.

2. Topology

Figure 1-3 Topology for sFlow Basic Functions



3. Notes

- Configure the L3 network reachable between the sFlow Agent and the sFlow Collector.
- Configure the sFlow function.

4. Procedure

Configure the L3 network reachable between the sFlow Agent and the sFlow Collector.

```
Device> enable
Device#configure terminal
Device(config)# interface GigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Device(config)# interface GigabitEthernet 0/2
Device(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
Device(config)# interface GigabitEthernet 0/3
Device(config-if-GigabitEthernet 0/1)# ip address 192.168.3.1 255.255.255.0
```

Configure 192.168.1.1 as the sFlow Agent address.

```
Device(config)# sflow agent address 192.168.1.1
```

Configure 192.168.3.100 as the address of sFlow Collector 1, and 6343 as the port number.

```
Device(config)# sflow collector 1 destination 192.168.3.100 6343
```

Configure the interface GigabitEthernet 0/1 to output flow samples and counter samples to sFlow Collector 1, and enable sFlow sampling on this interface.

```
Device(config)# interface GigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# sflow flow collector 1
Device(config-if-GigabitEthernet 0/1)# sflow counter collector 1
Device(config-if-GigabitEthernet 0/1)# sflow enable
```

5. Verification

Run the **show sflow** command to check whether the command output is consistent with the configuration.

```
Device# show sflow
sFlow datagram version 5
Global information:
Agent IP: 192.168.1.1
sflow counter interval:30
sflow flow max-header:64
sflow sampling-rate:8192
Collector information:
ID   IP                        Port Size VPN
1    192.168.3.100               6343 1400
2    NULL                      0    1400
Port information
Interface                    CID  FID  Enable
TenGigabitEthernet 0/1         1    1    B
```

Figure 1-4 shows the Top N tab of sFlowTrend, which displays the flow sampling result and the source IP addresses with the Top 5 traffic. The inbound traffic 450 kpps, and the outbound traffic is also 450 kpps, which is consistent with the actual traffic.

Figure 1-5 is the Counters tab of sFlowTrend, which displays the counter sampling result. The inbound traffic is 450 kpps, and the outbound traffic is also 450 kpps. All packets are unicast packets.

Figure 1-4 Flow Sampling Results

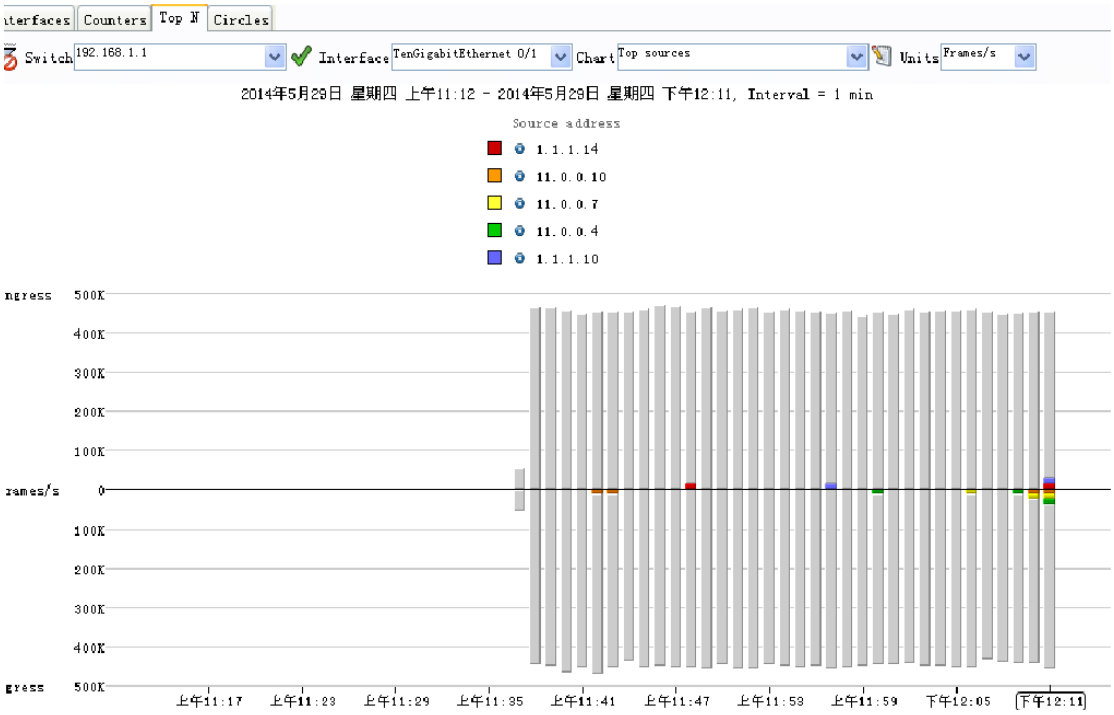
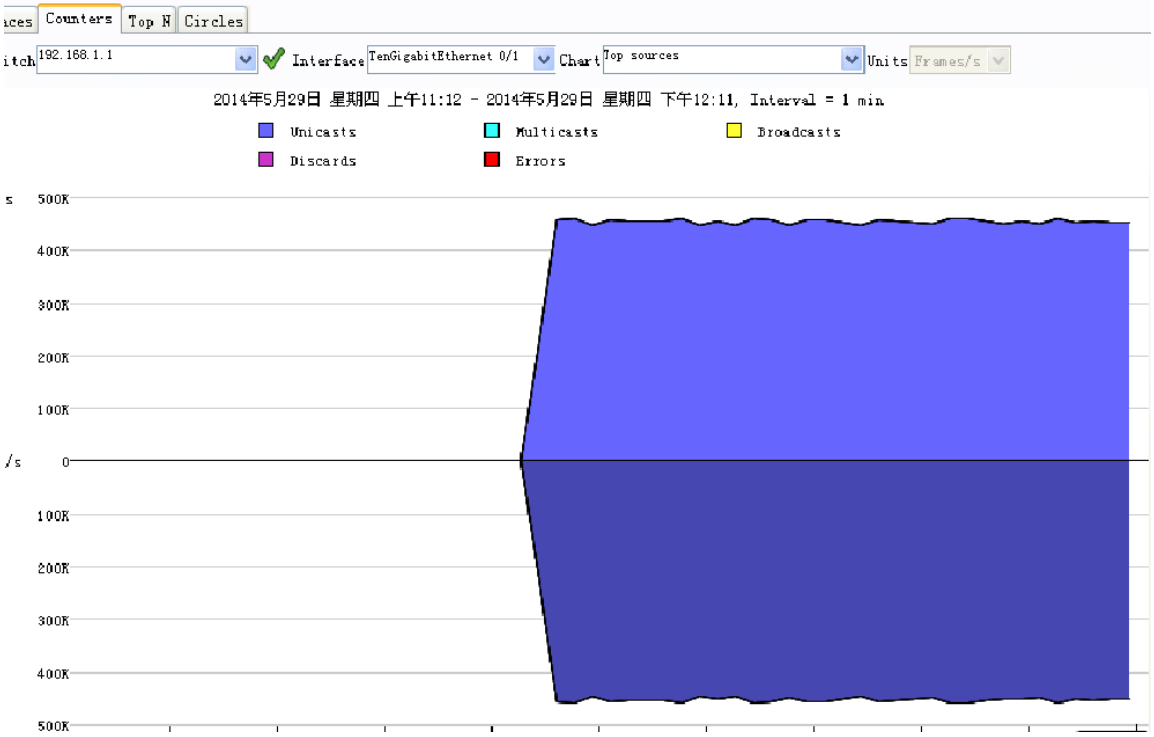


Figure 1-5 Counter Sampling Results



6. Configuration Files

Device configuration file

```
Hostname Device
!
sflow agent address 192.168.1.1
sflow collector 1 destination 192.168.3.100 6343
!
interface GigabitEthernet 0/1
 ip address 192.168.1.1 255.255.255.0
 sflow counter collector 1
 sflow flow collector 1
 sflow enable
!
interface GigabitEthernet 0/2
 ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet 0/3
 ip address 192.168.3.1 255.255.255.0
!
end
```

Contents

1 Configuring the Function of Displaying Device Restart Reasons 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Restrictions and Guidelines 1

1.3 Monitoring 1

1 Configuring the Function of Displaying Device Restart Reasons

1.1 Introduction

1.1.1 Overview

Diversified availability detection functions are implemented to ensure the availability of all system functions. While these functions ensure system availability by killing target processes or resetting cards, the following risks arise: The self-recovery behavior cannot be tracked or controlled in a unified manner. When a process is killed or a card is restarted, the service that triggers this self-recovery behavior cannot be located. If a process is frequently killed or a card is frequently reset due to the logic failure of a detection function, more serious system failure may occur. To solve these problems, a component is needed to track and control the service self-recovery behaviors of the system in a unified manner. The secondary protect and self-healing (PSH) module provides a method for users to check the device restart reason on the CLI interface. When a device restarts, you can view the device restart reasons by using the command provided by the PSH module on the device, eventually improving the availability and quality of the device.

1.1.2 Principles

The PSH module collects information about the process that triggers restart of the device before the device restarts, and saves the restart reason locally. You can either run a command on a device to view the locally stored restart reason of the device, or run a command on the primary device of a cluster to view the restart reasons of all devices in the cluster.

1.2 Restrictions and Guidelines

The PSH module records only self-healing events of the system, and service components cannot use it as an internal logging tool to record logs of the running process in a log file.

1.3 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring of the Function of Displaying Device Restart Reasons

Command	Purpose
show reboot-reason [**all**]	Displays the device restart reason.

Contents

1 Configuring NTP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 3
1.2 Restrictions and Guidelines 3
1.3 Configuration Task Summary 3
1.4 Configuring NTP Security Authentication 4
1.4.1 Overview 4
1.4.2 Restrictions and Guidelines 4
1.4.3 Procedure 4
1.5 Configuring NTP in Client/Server Mode 5
1.6 Configuring NTP-Related Parameters 5
1.6.1 Procedure 5
1.7 Configuring NTP Access Control 6
1.7.1 Overview 6
1.7.2 Restrictions and Guidelines 6
1.7.3 Procedure 6
1.8 Monitoring 7
1.9 Configuration Examples 7
1.9.1 Configuring the Local Clock Reference Mode of NTP 7
1.9.2 Configuring the External Clock Reference Mode of NTP 9

1.9.3 Configuring NTP Security Authentication 11

1.9.4 Configuring NTP Access Control Rights 13

1 Configuring NTP

1.1 Introduction

1.1.1 Overview

Network Time Protocol (NTP) is an application-layer protocol that enables network devices to synchronize time. NTP enables network devices to synchronize time with their servers or clock sources and provides high-precision time correction (the difference from the standard time is smaller than one millisecond in a LAN and smaller than decades of milliseconds in a WAN). In addition, NTP can prevent attacks by using encrypted acknowledgment. NTP is implemented based on the transport protocol, User Datagram Protocol (UDP), and the UDP port used is 123.

Currently, Ruijie devices can be used both as NTP clients and NTP servers. In other words, a Ruijie device can synchronize time with a time server, or act as a time server to provide time synchronization for other devices.

1.1.2 Principles

1. Basic Concepts

- NTP server

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

- NTP client

  A device synchronizes time with an NTP server in the network.

- **Stratum**

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

- Hardware Clock

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

2. NTP Principles

As shown in Figure 1-1, a client exchanges NTP packets with a server to implement time synchronization.

(1) The client sends a time synchronization request packet to all servers every 64 seconds.

(2) After receiving response packets from the servers, the client filters these response packets, and synchronizes time with an optimum server.

3. NTP Working Process

As shown in Figure 1-1, device B (B for short) acts as an NTP reference clock source, and device A (A for short) acts as an NTP client that synchronizes time with B. At a time point, the local clock of A is 19:00:00 and the local clock of B is 19:30:20.

(1) A sends an NTP request packet. The local time (T0) when the packet leaves from A is 19:00:00 and is filled in **Originate Timestamp**.

(1) After a network delay of 2s, the local time (T1) when B receives the request packet is 19:30:23 and is filled in **Receive Timestamp**.

(2) B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from B is 19:30:24 and is filled in **Transmit Timestamp**.

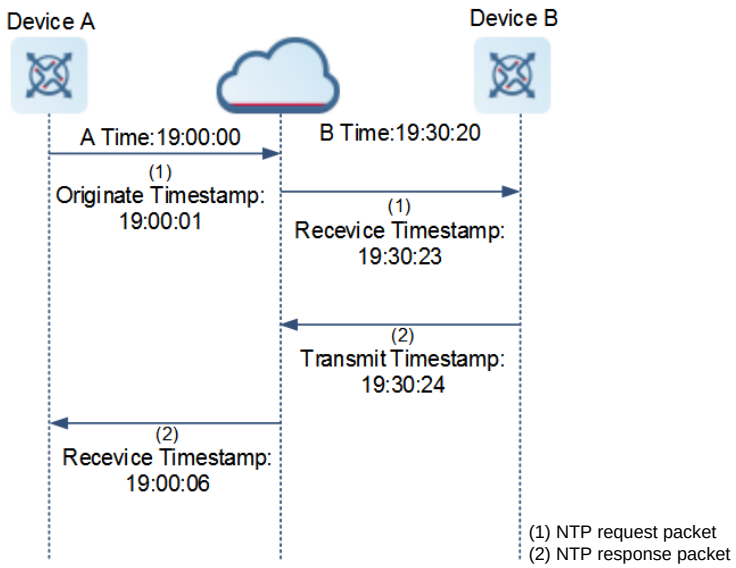
(3) After a network delay of 2s, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

The specific calculations for time synchronization are as follows:

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

b A obtains the packet round-trip delay of 4 seconds between A and B by using the formula (T3-T0)-(T2-T1).

Figure 1-1 NTP Principles



- NTP working mode
  - External clock reference mode: In this mode, a device acts as both a server and a client. If receiving time synchronization requests from other clients, the device must synchronize time with the specified server, and then provide the time synchronization service for the clients only after successful synchronization with the specified server.
  - Local clock reference mode: In this mode, a device uses the default local clock as the reliable clock source and provides the time synchronization service directly for other clients.

4. NTP Security Mechanism

To prevent malicious damage to the time server and improve the security of time synchronization, NTP provides security authentication and access control functions.

- Security authentication

  NTP uses the authentication mechanism to check whether the time synchronization information really comes from the announced server and check the information return path to provide an anti-interference protection mechanism.

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

- NTP access control using the kiss-o-death (KoD) packet

  NTP provides a minimum security measure by using an ACL. Normally, the denial-of-service packets are discarded, and there is no operation other than incrementing the statistics counter. Sometimes a more proactive response is required. For example, the client is explicitly requested to stop sending packets to the server and to leave a message for the system operator. Therefore, open-source NTP proposes a KoD packet, which can be used to respond to special processing of the client when access control is configured on the server.

  The format of a KoD packet is the same as that of a common NTP packet, except that the **Leap Indicator** field is set to **clock unsynchronized**, the **Stratum** field is set to **0**, and the **Reference ID** field is set to a 4-byte ASCII code. The code is "RATE" if the limited flag is set and the rate threshold is exceeded. After the NTP client receives the KoD packet with the code "RATE", it limits the rate according to the minimum interval specified in the packet.

1.1.3 Protocols and Standards

- RFC 1305: Network Time Protocol (Version 3)
- RFC 5905: Network Time Protocol (Version 4)

1.2 Restrictions and Guidelines

- You cannot configure both the NTP and SNTP functions on the same device.
- Only L3 interfaces support NTP.
- To ensure accuracy of time synchronization, avoid configuring two or more clock sources whenever possible to prevent clock flapping.
- You can run the **ntp service disable** command to disable the NTP server function so that the device acts only as a client. This command cannot be configured together with **ntp master**.

1.3 Configuration Task Summary

NTP configuration includes the following tasks:

(1) (Optional) Configuring NTP Security Authentication

(2) Configuring NTP in Client/Server Mode

(3) (Optional) Configuring NTP-Related Parameters

(4) (Optional) Configuring NTP Access Control

1.4 Configuring NTP Security Authentication

1.4.1 Overview

- Synchronizing time from a trusted reference clock source: Use a device as a client to synchronize time only from a trusted external reference clock source to the local clock.
- Providing time synchronization for a trusted device: Use the local clock of a device as the NTP reference clock source to provide time synchronization for only a trusted device.

1.4.2 Restrictions and Guidelines

- The authentication keys of the client and server must be the same.
- To provide time synchronization for a trusted device, you must specify a trusted authentication key by using the key ID. Only one trusted key can be configured. The specified authentication key must be consistent with that of the trusted device.
- To synchronize time with a trusted reference clock source, you must specify a trusted authentication key by using the key ID. Each trusted reference clock source is mapped to an authentication key. The authentication keys must be consistent with the keys of trusted reference clock sources.
- By default, a client does not use a global security authentication mechanism. If no security authentication mechanism is used, communication will not be encrypted. A global security indicator is not enough to imply that the communication between the client and server is implemented in an encrypted manner. Other global keys and an encryption key for the server must also be configured for initiating encrypted communication between the client and server.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a global security authentication mechanism for NTP.

ntp authenticate

(4) Configure a global authentication key for NTP.

ntp authentication-key *authentication-key-id* **md5** *authentication-key-string* [*enc-type*]

The NTP global authentication mechanism is disabled by default.

(5) (Optional) Configure a globally trusted key ID for NTP.

ntp trusted-key *trusted-key-id*

(6) (Optional) Configure an authentication key ID for an external reference clock source.

ntp server [**oob** | **vrf** *vrf-name*] { *ipv4-addr* | *ipv6-address* | *peer-hostname* | **ip** *domain* | **ipv6** *domain* } [**version** *version*] [**source** *interface-type interface-number*] [**key** *keyid*] [**prefer**] [**via** *mgmt-name*]

By default, no authentication key ID is configured for an external reference clock source.

1.5 Configuring NTP in Client/Server Mode

1. Overview

This section describes how to configure a device as a client to synchronize time from an external reference clock source to the local clock. After successful time synchronization, the device can act as a time synchronization server to provide the time synchronization service.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an NTP server.

ntp server [**oob** | **vrf** *vrf-name*] { *ipv4-address* | *ipv6-address* | *peer-hostname* | **ip** *domain* | **ipv6** *domain* } [**version** *version*] [**source** *interface-type interface-number*] [**key** *keyid*] [**prefer**] [**via** *mgmt-name*]

No NTP server is configured by default.

1.6 Configuring NTP-Related Parameters

1.6.1 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the interval for time synchronization with the external server.

ntp interval *synchronization-interval-time*

By default, the NTP synchronization interval is 64s.

(4) (Optional) Configure automatic update of the hardware clock.

ntp update-calendar

Automatic update of the hardware clock is not configured by default.

(5) (Optional) Configure the NTP master clock.

ntp master [*stratum*]

The NTP master clock is disabled by default.

stratum: specifies the stratum of a local clock, ranging from 1 to 15. The default value is 8.

(6) (Optional) Disable the NTP time synchronization service provided for other devices.

ntp service disable

The NTP time synchronization service is enabled by default.

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) (Optional) Disable receiving of NTP packets on an interface.

ntp disable

The function of receiving NTP packets on an interface is enabled by default.

1.7 Configuring NTP Access Control

1.7.1 Overview

NTP access control provides a minimum security measure. A more secure method is to use the NTP authentication mechanism.

1.7.2 Restrictions and Guidelines

- If no access control rule is configured, all NTP services can be accessed. If access control rules are configured, only NTP services that comply with the access control rules can be accessed.
- The system currently does not support the access control query function.
- If the packet request interval of the NTP client is smaller than that allowed by the server, the NTP server discards the packets. This function takes effect only after the **ntp access-group limited access-list-number** | **access-list-name** [**kod**] command is configured. When the KoD-enabled NTP device acts as a client, it reduces the rate after receiving a KoD packet. A KoD-disabled device does not reduce the rate. Note that KoD cannot be triggered by specifying the interval in the **ntp interval** command.
- You can run the **ntp discard** command to configure the packet request interval allowed by the server. If the packet request interval of the NTP client is smaller than that allowed by the server, the NTP server discards the packets. This function takes effect only after the **ntp access-group limited access-list-number** | **access-list-name** [**kod**] command is configured.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the NTP access control rights.

ntp access-group { **limited** | **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name* [**kod**]

No NTP access control rule is configured by default.

(4) (Optional) Configure the minimum packet interval allowed by NTP.

ntp discard min-spacing *discard-min-spacing-interval* **avg-spacing** *avg-spacing-interval*

By default, the minimum packet request interval allowed by NTP is 2s, and the average packet request interval is 8s.

1.8 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 NTP Monitoring

Command	Purpose
show ntp status	Displays the current NTP information.
show ntp packets	Displays the sent and received NTP packets.
show ntp server	Displays the NTP server information.
show ntp server	Displays the NTP server list.
debug ntp	Debugs the DNS function.
no debug ntp	Disables the debugging function.

1.9 Configuration Examples

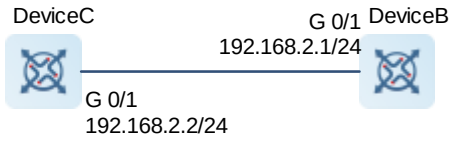
1.9.1 Configuring the Local Clock Reference Mode of NTP

1. Requirements

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

2. Topology

Figure 1-2 Local Clock Reference Mode of NTP



3. Notes

- Configure the local clock of device B as the NTP reference clock source.
- Device C synchronizes time from device B.

4. Procedure

Set the IP address of GigabitEthernet 0/1 on device B to 192.168.2.1/24.

```
DeviceB> enble
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of GigabitEthernet 0/1 on device C to 192.168.2.2/24.

```
DeviceC> enble
DeviceC# configure terminal
DeviceC(config)# interface gigabitEthernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/1)# exit
```

Configure device B as the NTP server.

```
DeviceB(config)# ntp master
```

Enable the NTP function on device C.

```
DeviceC> enble
DeviceC# configure terminal
DeviceC(config)# ntp server 192.168.2.1
DeviceC(config)# ntp enable
```

5. Verification

Run the **ping** command to verify L3 reachability between device B and device C.

```
DeviceB# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **clock set** command to modify the time on device B.

```
DeviceB# clock set 11:00:00
Set system clock: 11:00:00 UTC Fri, Feb 26, 2021
```

Run the **show clock** command on device C to check whether time synchronization is successful.

```
DeviceC# show clock
11:00:01 UTC Fri, Feb 26, 2021
```

6. Configuration Files

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
ntp master
```

```
!
end
```

- Device C configuration file

```
hostname DeviceC
!
ntp server 192.168.2.1
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
!
end
```

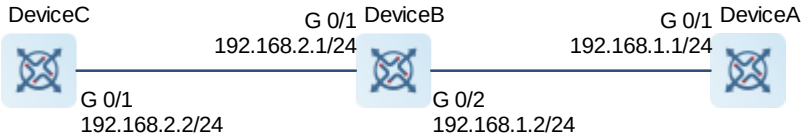
1.9.2 Configuring the External Clock Reference Mode of NTP

1. Requirements

Use a device as a client to synchronize time from an external reference clock source to the local clock. After successful time synchronization, the device can act as a time synchronization server to provide the time synchronization service.

2. Topology

Figure 1-3 Topology for the External Clock Reference Mode of NTP



3. Notes

- Configure the NTP external clock reference mode on device B.
- Configure device A as the reference clock source of device B.
- Device C synchronizes time from device B.

4. Procedure

Set the IP address of GigabitEthernet 0/1 on device A to 192.168.1.1/24.

```
DeviceA> enble
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of GigabitEthernet 0/1 on device B to 192.168.2.1/24, and the IP address of GigabitEthernet 0/2 to 192.168.1.2/24.

```
DeviceB> enble
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
```

```
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
DeviceB(config)# interface gigabitEthernet 0/2
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of GigabitEthernet 0/1 on device C to 192.168.2.2/24.

```
DeviceC> enble
DeviceC# configure terminal
DeviceC(config)# interface gigabitEthernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/1)# exit
```

Configure device A as the reference clock source of device B.

```
DeviceA(config)# ntp master
```

Configure the NTP external clock reference mode on device B.

```
DeviceB(config)# ntp server 192.168.1.1
```

Enable device C to synchronize time from device B.

```
DeviceC(config)# ntp server 192.168.2.1
```

5. Verification

Run the **ping** command to verify L3 reachability between device B and device A.

```
DeviceB# ping 192.168.1.1
Sending 5, 100-byte ICMP Echoes to 192.168.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **ping** command to verify L3 reachability between device B and device C.

```
DeviceB# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **show ntp status** command to display the NTP configuration.

```
DeviceB# sh ntp status
Clock is synchronized, stratum 9, reference is 192.168.1.1
nominal freq is 250.000 Hz, actual freq is 250.000 Hz, precision is 2**18
reference time is E3527947.D5254A29 (14:03:51.000 UTC Sun, Nov 8, 2020)
clock offset is -0.00012 sec, root delay is 0.00282 sec
root dispersion is 0.01153 msec, peer dispersion is 0.00025 msec
system poll interval is 64, last update was 43 sec ago
system time(GMT) is E3527973.740AB522 (14:04:35.000 GMT Sun, Nov 8, 2020)
```

Run the **clock set** command to modify the time on device A.

```
DeviceA# clock set 11:00:00
```

```
Set system clock: 11:00:00 UTC Fri, Feb 26, 2021
```

Run the **show clock** command on device B to check whether time synchronization is successful.

```
DeviceB# show clock
11:00:01 UTC Fri, Feb 26, 2021
```

Run the **show clock** command on device C to check whether time synchronization is successful.

```
DeviceC# show clock
11:00:01 UTC Fri, Feb 26, 2021
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 ip address 192.168.1.1 255.255.255.0
ntp master
!
end
```

- Device B configuration file

```
hostname DeviceB
!
ntp server 192.168.1.1
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
!
interface GigabitEthernet 0/2
 ip address 192.168.1.2 255.255.255.0
!
end
```

- Device C configuration file

```
hostname DeviceC
!
ntp server 192.168.2.1
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
!
end
```

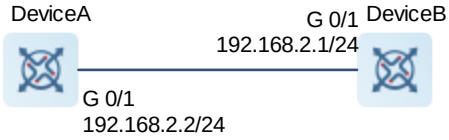
1.9.3 Configuring NTP Security Authentication

1. Requirements

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

2. Topology

Figure 1-4 Topology for NTP Security Authentication



3. Notes

- Configure device A as the reference clock source of device B, enable device A to provide device B with the NTP service that requires security authentication, and set the authentication key to "abcd".

4. Procedure

Set the IP address of GigabitEthernet 0/1 on device A to 192.168.2.2/24.

```
DeviceA> enble
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of GigabitEthernet 0/1 on device B to 192.168.2.1/24.

```
DeviceB> enble
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure device A as the reference clock source of device B, enable device A to provide device B with the NTP service that requires security authentication, and set the authentication key to "abcd".

```
DeviceB(config)# ntp authenticate
DeviceB(config)# ntp authentication-key 1 md5 abcd
DeviceB(config)# ntp trusted-key 1
DeviceB(config)# ntp server 192.168.2.2
```

5. Verification

Run the **ping** command to verify L3 reachability between device B and device A.

```
DeviceB# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **clock set** command to modify the time on device A.

```
DeviceA# clock set 11:00:00
Set system clock: 11:00:00 UTC Fri, Feb 26, 2021
```

Run the **show clock** command on device B to check whether time synchronization is successful.

```
DeviceB# show clock
11:00:01 UTC Fri, Feb 26, 2021
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
ntp master
!
end
```

- Device B configuration file

```
hostname DeviceB
!
ntp authentication-key 1 md5 abcd
ntp authenticate
ntp trusted-key 1
ntp server 192.168.2.2
!
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
!
end
```

1.9.4 Configuring NTP Access Control Rights

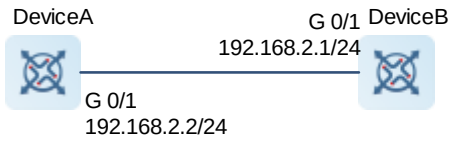
1. Requirements

Configure the access control function to prevent malicious damage to the time server and improve the security of time synchronization.

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

2. Topology

Figure 1-5 Topology for Implementing NTP Access Control Rights



3. Procedure

Set the IP address of GigabitEthernet 0/1 on device A to 192.168.2.2/24.

```
DeviceA> enble
```

```
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of GigabitEthernet 0/1 on device B to 192.168.2.1/24.

```
DeviceB> enble
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure device A as the reference clock source of device B. Allow only the device with the IP address of 192.168.2.2 to send a time synchronization request to the local device.

```
DeviceB(config)# ntp server 192.168.2.2
DeviceB(config)# access-list 1 permit host 192.168.2.2
DeviceB(config)# ntp access-group serve-only 1
```

Configure device A as the NTP server, limit the request packet interval of the client, and send KoD packets.

```
DeviceA(config)# ip access-list standard limited1
DeviceA(config-std-nacl)# 10 permit any
DeviceA(config)# exit
DeviceA(config)# ntp access-group limited limited1 kod
DeviceA(config)# ntp discard min-spacing 5 avg-spacing 5
DeviceA(config)# ntp master
```

4. Verification

Run the **ping** command to verify L3 reachability between device B and device A.

```
DeviceB# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **clock set** command to modify the time on device A.

```
DeviceA# clock set 11:00:00
Set system clock: 11:00:00 UTC Fri, Feb 26, 2021
```

Run the **show clock** command on device B to check whether time synchronization is successful.

```
DeviceB# show clock
11:00:01 UTC Fri, Feb 26, 2021
```

5. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip access-list standard limited1
 10 permit any
```

```
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
ntp master
ntp access-group limited limited1 kod
!
end
```

- Device B configuration file

```
hostname DeviceB
!
ip access-list standard 1
 10 permit 192.168.2.2
!
ntp server 192.168.2.2
ntp access-group serve-only 1
!
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
!
end
```

Contents

1 Configuring SNTP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 2
1.2 Restrictions and Guidelines 2
1.3 Configure SNTP 2
1.3.1 Overview 2
1.3.2 Restrictions and Guidelines 2
1.3.3 Procedure 2
1.4 Monitoring 3
1.5 Configuration Examples 3
1.5.1 Configuring Basic Functions of SNTP 3

1 Configuring SNTP

1.1 Introduction

1.1.1 Overview

NTP uses a complex algorithm for time synchronization, and raises high requirements for the system. As a simplified version of NTP, Simple Network Time Protocol (SNTP), inherits the protocol specification and implementation process of NTP, and adopts the same packet format and interaction mode as NTP. By setting some fields in the packet to predetermined values, SNTP simplifies the time synchronization algorithm and lowers the requirements for system performance. Although the precision of SNTP time synchronization is compromised while the algorithm is simplified, SNTP can generally achieve a precision of about 1s. Therefore, when the time precision requirements are not very high, you can choose to use SNTP. SNTP packets are the same as NTP packets, and therefore the SNTP client is fully compatible with the NTP server.

1.1.2 Principles

Like NTP, SNTP also uses the client/server mode for SNTP/NTP message interaction. The client sends a time synchronization packet to the server at a certain interval (half an hour by default). After receiving a response packet from the server, the client synchronizes time.

As shown in Figure 1-1, device B (B for short) acts as an NTP reference clock source, device A (A for short) acts as an SNTP client that synchronizes time with B. At a time point, the local clock of A is 19:00:00 and the local clock of B is 19:30:20.

(1) A sends an SNTP/NTP request packet. The local time (T0) when the packet leaves from A is 19:00:00 and is filled in Originate Timestamp.

(2) After a network delay of 2s, the local time (T1) when B receives the request packet is 19:30:23 and is filled in Receive Timestamp.

(3) B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from B is 19:30:24 and is filled in Transmit Timestamp.

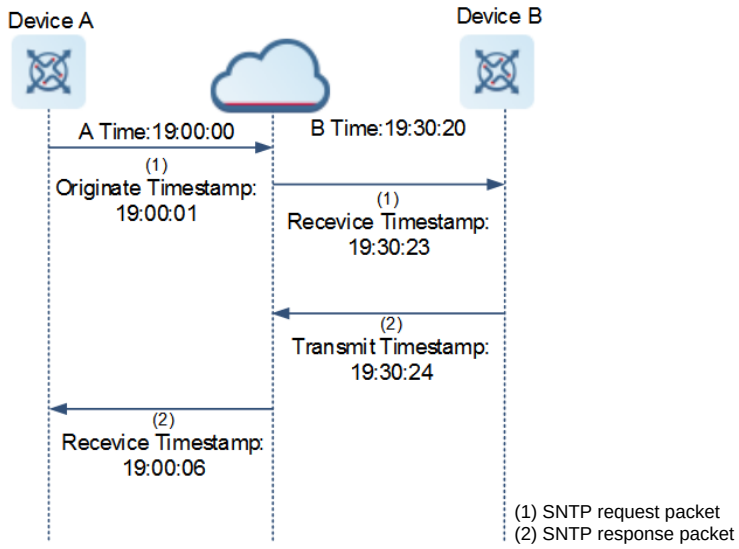
(4) After a network delay of 2s, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

The specific calculations for time synchronization are as follows:

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

b A obtains the packet round-trip delay of 4 seconds between A and B by using the formula (T3-T0)-(T2-T1).

Figure 1-1 SNTP Principles



1.1.3 Protocols and Standards

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

1.2 Restrictions and Guidelines

You cannot configure both the NTP and SNTP functions on the same device.

1.3 Configuring SNTP

1.3.1 Overview

An SNTP client accesses an NTP server regularly to calibrate the clock.

1.3.2 Restrictions and Guidelines

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

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable SNTP.

sntp enable

The SNTP function is disabled by default.

(4) Configure the IP address of an SNTP server.

sntp server [**oob**] { *ipv4-address* | *domain* } [**via** *mgmt-name*] [**source** *source-ipv4-address*]

No SNTP server is configured by default.

(5) (Optional) Configure the SNTP time synchronization interval.

sntp interval *synchronization-interval-time*

The default interval for clock synchronization between an SNTP client and SNTP/NTP server is 1800s.

1.4 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 SNTP Monitoring

Command	Purpose
show sntp	Displays SNTP-related parameters.
debug sntp	Debugs the DNS function.

1.5 Configuration Examples

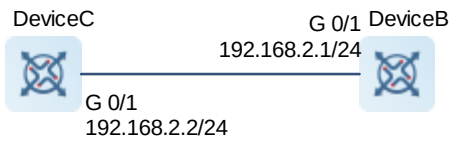
1.5.1 Configuring Basic Functions of SNTP

1. Requirements

- Use the local clock of device B as the NTP reference clock source to provide time synchronization for device C.
- Use device C as an SNTP client to synchronize time from device B.

2. Topology

Figure 1-2 Topology for Implementing SNTP Basic Functions



3. Notes

- Configure device B as the SNTP server of device C.

- Enable the SNTP function on device C.

4. Procedure

Set the IP address of GigabitEthernet 0/1 on device B to 192.168.2.1/24.

```
DeviceB> enble
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of GigabitEthernet 0/1 on device C to 192.168.2.2/24.

```
DeviceC> enble
DeviceC# configure terminal
DeviceC(config)# interface gigabitEthernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/1)# exit
```

Configure device B as the NTP server.

```
DeviceB(config)# ntp master
```

Enable the SNTP function on device C.

```
DeviceC(config)# sntp server 192.168.2.1
DeviceC(config)# sntp enable
```

5. Verification

On device B, run the **ping** command to verify L3 reachability between device B and device C.

```
DeviceB# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

On device C, run the **show sntp** command to display the SNTP status and check whether the server is successfully configured.

```
DeviceC# show sntp
 SNTP state           : Enable
 SNTP oob mode        : Enable
 SNTP server          : 192.168.2.1
 SNTP sync interval    : 1800
 Time zone            : -0
```

Run the **clock set** command to modify the time on device B.

```
DeviceB# clock set 11:00:00
Set system clock: 11:00:00 UTC Fri, Feb 26, 2021
```

Run the **show clock** command on device C to check whether time synchronization is successful.

```
DeviceC# show clock
11:00:01 UTC Fri, Feb 26, 2021
```

6. Configuration Files

- Device B configuration file

```
DeviceB# show running-config
hostname DeviceB
!
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
ntp master
!
end
```

- Device C configuration file

```
DeviceC# show running-config
hostname DeviceC
!
sntp server 192.168.2.2
sntp enable
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
!
end
```

Contents

1 Configuring the FTP Server 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 3
1.2 Configuration Task Summary 3
1.3 Configuring Basic Functions of the FTP Server 3
1.3.1 Overview 3
1.3.2 Procedure 3
1.4 Configuring FTP Session Management 4
1.4.1 Overview 4
1.4.2 Procedure 4
1.5 Configuring the FTP Lock Function 5
1.5.1 Overview 5
1.5.2 Restrictions and Guidelines 5
1.5.3 Procedure 5
1.6 Enabling AAA on the FTP Server 6
1.6.1 Overview 6
1.6.2 Restrictions and Guidelines 6
1.6.3 Prerequisites 6
1.6.4 Procedure 6
1.7 Configuring Read/Write Permission Control of FTP Users 6

1.7.1 Overview 6

1.7.2 Procedure 6

1.8 Monitoring 7

1.9 Configuration Examples 7

1.9.1 Providing the FTP Service in a LAN 7

1 Configuring the FTP Server

1.1 Introduction

1.1.1 Overview

File Transfer Protocol (FTP) is a standard application layer protocol formulated by the IETF Network Working Group. It implements file transfer based on Transmission Control Protocol (TCP). FTP is a major method for transferring files on the Internet.

FTP adopts the client/server model. As shown in Figure 1-1, a device can act as an FTP server to provide remote client access and program operations. By issuing commands to the server through the client, you can view the files in the FTP server directory, copy files from a remote computer to the local device, and transfer local files to the server. In addition, FTP provides functions, such as login authentication and read/write access control.

Figure 1-1 FTP Client/Server Mode

1.1.2 Principles

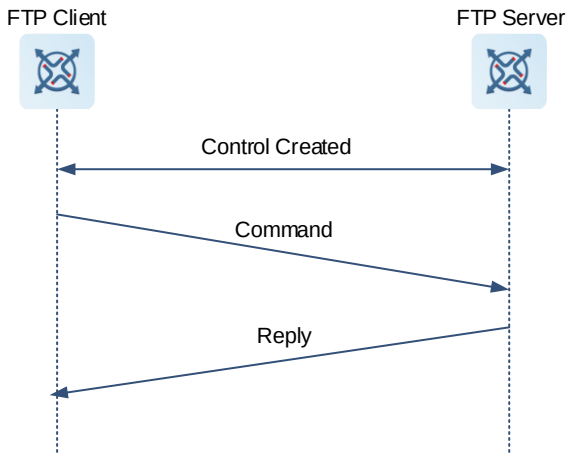
1. FTP Connection

FTP sets up two TCP connections between the client and the server, namely the control connection and the data connection.

- The control connection uses port 21 to transmit control commands, and is always in enabled state.
- The data connection uses port 20 to transmit data. The server can proactively enable or disable the data connection. It sets up a new data connection every time a file or directory is transferred.

For some simple sessions, only the control connection needs to be enabled, the client sends a command to the server, and the sever returns a response after receiving the command. The process is shown in Figure 1-2.

Figure 1-2 Control Connection



When the client sends a command for uploading or downloading data, both the control connection and data connection must be established.

2. User Login and Authentication

To access files on the FTP server, the FTP client must have a user account authorized by the FTP server. By default, a device supports configuration of up to 10 users, 2 connections per user, and 10 connections with the server.

In addition, the read and write permissions of files can be defined to effectively prevent unauthorized users from accessing internal files. When the number of a user's FTP login failures reaches the upper limit, the IP address or username used for login is locked. Within a certain period of time, all users cannot log in to the FTP server properly using this IP address or username.

3. Supported FTP Commands

After receiving an FTP connection request, the FTP server requires the client to provide the username and password for authentication.

If the client passes the authentication, the FTP client commands can be executed. The following table lists the FTP client commands supported by the FTP server.

Table 1-1 FTP Client Commands Supported by the FTP Server

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

For how to use these FTP client commands, refer to the documentation of the FTP client software used. In addition, many FTP client tools, such as CuteFTP and FlashFXP, provide the graphic user interface (GUI), which allows users to perform operations without configuring FTP commands.

1.1.3 Protocols and Standards

- RFC959: File Transder Protocol (FTP)
- RFC3659: Extensions to FTP
- RFC2228: FTP Security Extensions
- RFC2428: FTP Extensions for IPv6 and NATs
- RFC1635: How to Use Anonymous FTP

1.2 Configuration Task Summary

FTP server configuration includes the following tasks:

(1) Configuring Basic Functions of the FTP Server

(2) (Optional) Configuring FTP Session Management

(3) (Optional) Configuring the FTP Lock Function

(4) (Optional) Enabling AAA on the FTP Server

(5) (Optional) Configuring Read/Write Permission Control of FTP Users

1.3 Configuring Basic Functions of the FTP Server

1.3.1 Overview

This section describes how to enable the FTP server and configure the username, password, and top-level directory to provide the FTP service for the FTP client.

1.3.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the FTP server.

ftp-server enable

The FTP server is disabled by default.

(4) Configure the top-level directory of the FTP server.

ftp-server topdir *directory*

By default, no top-level directory under which the FTP client can read and write files is configured, that is, the client is prohibited from accessing any directory on the FTP server.

(5) Configure a username and password for server login.

ftp-server username *username* [**privilege level**] **password** [*type*] *password*

By default, no username and password are configured for login to the FTP server, that is, no login users are restricted.

1.4 Configuring FTP Session Management

1.4.1 Overview

- The FTP login times refers to the number of times that the user's account and password can be verified when the user logs in to the FTP server.
- The FTP login timeout refers to the maximum time that the user can stay online after the username and password are verified. If the username and password are not verified again before login timeout, the session will be terminated to ensure that other users can log in to the FTP server.
- The idle timeout refers to the time from the completion of the last FTP operation to the start of the next FTP operation in an FTP session. After the server responds to an FTP client command (for example, after a file is completely transferred), the server starts to count the idle time again, and stops counting when the next FTP client command arrives. Therefore, the configuration of the idle timeout does not affect time-consuming file transfer operations.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure FTP session management. Configure at least one of the following tasks.

- Configure the FTP login times.

  ftp-server login times *times*

  By default, the FTP login times is 3, that is, a session will be terminated once you enter an incorrect username or password so that other users can go online.

- Configure the FTP login timeout.

  ftp-server login timeout *time*

  By default, the FTP login timeout is 2 minutes.

- Configure the idle timeout.

  ftp-server timeout *time*

  By default, the idle timeout of an FTP session is 10 minutes.

- Configure the maximum number of FTP sessions.

  ftp-server max-sessions *number*

  By default, the maximum number of FTP sessions is 20.

1.5 Configuring the FTP Lock Function

1.5.1 Overview

- After the IP address lock function is enabled, if the cumulative number of login failures caused by entry of the incorrect username or password reaches the configured upper limit, the FTP session is terminated and the user's IP address is locked. In addition, all users cannot log in to the FTP server properly using this IP address or username.
- After the username lock function is enabled, if the cumulative number of login failures caused by entry of the incorrect password reaches the configured upper limit, the FTP session is terminated and the username is locked. The user cannot log in to the FTP server, but other users are not affected.
- The FTP lock time refers to the duration that a user needs to wait for automatic unlocking after the user is locked because the number of the user's login failures reaches the upper limit. The locked user can log in to the FTP server only after the login silence time expires.
- The maximum number of login verification times allowed by the FTP lock function refers to the maximum number of times that the username and password of a user can be verified after the FTP lock function is enabled. The default value is 3. If the number of verification failures exceeds the configured upper limit, the session is terminated and the user is locked.

1.5.2 Restrictions and Guidelines

After the IP address lock function is enabled, if the number of locked IP addresses reaches the upper limit, the full lock function is enabled. Then, the FTP server no longer accepts the connection request from any user until the number of locked IP addresses is smaller than the upper limit.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the FTP lock function. Configure at least one of the following tasks.

- Disable the IP address lock function.

  ftp-server login ip-block disable

  The IP address lock function is enabled by default.

- Configure the username lock function.

  ftp-server login username-block disable

  The username lock function is enabled by default.

- Configure the FTP lock time.

  ftp-server login silence-time *time*

  By default, the FTP lock time is 5 minutes.

- Configure the maximum number of IP addresses that can be locked after the IP address lock function is enabled.

ftp-server login max-block-limit *limit*

By default, up to 30 IP addresses can be locked.

1.6 Enabling AAA on the FTP Server

1.6.1 Overview

By default, FTP does not support AAA login authentication. However, you can enable AAA on the FTP server through configuration.

1.6.2 Restrictions and Guidelines

This command takes effect only after FTP is enabled.

1.6.3 Prerequisites

Enable the AAA function before configuring this command. For details about how to enable AAA, see "Configuring AAA" in *Security Configuration Guide*.

1.6.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA on the FTP server.

ftp-server authentication { **default** | *name* }

By default, FTP does not support AAA login authentication.

1.7 Configuring Read/Write Permission Control of FTP Users

1.7.1 Overview

After the user read/write permission control function is enabled, the configured FTP user levels or AAA username levels can be used to control read/write permissions. By default, users of all levels have the read/write permissions. After permission control is enabled, if the user level is not configured, it is set to 1 by default and the user has only the read permission, that is, the user can only download data. You can configure FTP users of different levels as required for read/write permission control.

1.7.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable read/write permission control of FTP users.

ftp-server login permission enable

By default, read/write permission control of FTP users is disabled.

1.8 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

Running the **clear** command may lose vital information and thus interrupt services.

Table 1-2 FTP Server Monitoring

Command	Purpose
clear ftp-server block-list [**all** | **ip-address** { *ipv4-address* | *ipv6-address* } [**vrf** *vrf_name*] | **username** *user*]	Clears the user lock entries in the FTP lock list.
show ftp-server	Displays the FTP server status information.
show ftp-server { **ip-block** | **username-block** } **list**	Displays the user lock entries in the FTP lock list.
debug ftp-server err	Debugs the FTP server error events.
debug ftp-server pro	Debugs the FTP server message events.

1.9 Configuration Examples

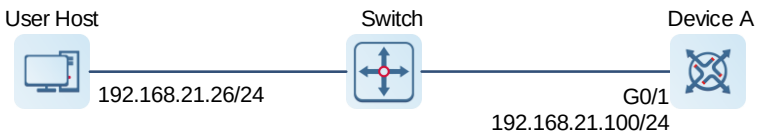
1.9.1 Providing the FTP Service in a LAN

1. Requirements

As shown in Figure 1-3, a device in a LAN acts as the FTP server to provide the upload and download services for users. The switch is an access device. The required session idle timeout is 5 minutes.

2. Topology

Figure 1-3 Providing the FTP Service in a LAN



3. Notes

Configure device A as follows:

(1) Enable the FTP server function.

(2) Configure the top-level directory **/syslog**.

(3) Set the username to **user** and password to **password**.

(4) Set the session idle timeout to **5** minutes.

4. Procedure

(1) Configure device A.

a. Configure an IP address.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1DeviceA(config-if-GigabitEthernet
0/1)# ip address 192.168.21.100 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

b. Enable the FTP server function.

```
DeviceA(config)# ftp-server enable
```

c. Configure the top-level directory **/syslog**.

```
DeviceA(config)# ftp-server topdir /syslog
```

d. Set the username to **user** and password to **password**.

```
DeviceA(config)# ftp-server username user password password
```

e. Set the session idle timeout to **5** minutes.

```
DeviceA(config)# ftp-server timeout 5
```

(2) Configure the user host.

Set the IP address of the user host to 192.168.21.26/24.

5. Verification

Run the **show ftp-server** command to view the FTP server configurations.

```
DeviceA# show ftp-server
   ftp-server information
===================================
enable : Y
```

```
topdir : /syslog
timeout: 5min
total connect: 0
username:user
password:(PLAINT)password
connect num[0]
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface gigabitEthernet 0/1
ip address 192.168.21.100 255.255.255
!
ftp-server enable
ftp-server topdir /syslog
ftp-server timeout 5
ftp-server username user password password
!
```

7. Common Errors

- No username is configured.
- No password is configured.
- No top-level directory is configured.

Contents

1 Configuring FTP Client 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 3
1.2 Configuration Task Summary 3
1.3 Enabling the FTP Client to Upload Files 3
1.3.1 Overview 3
1.3.2 Restrictions and Guidelines 4
1.3.3 Prerequisites 4
1.3.4 Procedure 4
1.4 Enabling the FTP Client to Download Files 4
1.4.1 Overview 4
1.4.2 Restrictions and Guidelines 4
1.4.3 Prerequisites 4
1.4.4 Procedure 4
1.5 Configuring the FTP Connection Mode 5
1.5.1 Overview 5
1.5.2 Restrictions and Guidelines 5
1.5.3 Procedure 5
1.6 Configuring the Transmission Mode of the FTP Client 5
1.6.1 Overview 5

1.6.2 Restrictions and Guidelines 5

1.6.3 Procedure 5

1.7 Configuring the Source IP Address for FTP Connection 6

1.7.1 Overview 6

1.7.2 Restrictions and Guidelines 6

1.7.3 Procedure 6

1.8 Monitoring 6

1.9 Configuration Examples 7

1.9.1 Configuring the FTP Client 7

1 Configuring FTP Client

1.1 Introduction

1.1.1 Overview

File Transfer Protocol (FTP) is an application of TCP/IP. By setting up a connection-oriented and reliable TCP connection between the FTP client and server, a user can access a remote computer that runs the FTP server program.

An FTP client enables file transfer between a device and the FTP server over FTP. A user uses the client to send a command to the server. The server responds to the command and sends the execution result to the client. By means of command interaction, the user can view files in the server directory, copy files from a remote computer to a local computer, and transfer local files to a remote computer.

FTP facilitates sharing of program/data files and remote use of computers. Users can transfer data in an efficient and reliable manner without caring about differences between files systems on different hosts.

A Ruijie FTP client runs interactive commands in a way different from a standard FTP client. You enter the copy command in the CLI to automatically run commands related to the control connection, such as **open**, **user**, and **pass**. After a control connection is established, the file transfer process starts. Then, a data connection is established to upload or download files.

Note

For the principles of the connection between the FTP client and server, see "Configuring FTP Server" in *IP Service Configuration Guide*.

The following sections introduce only the FTP client.

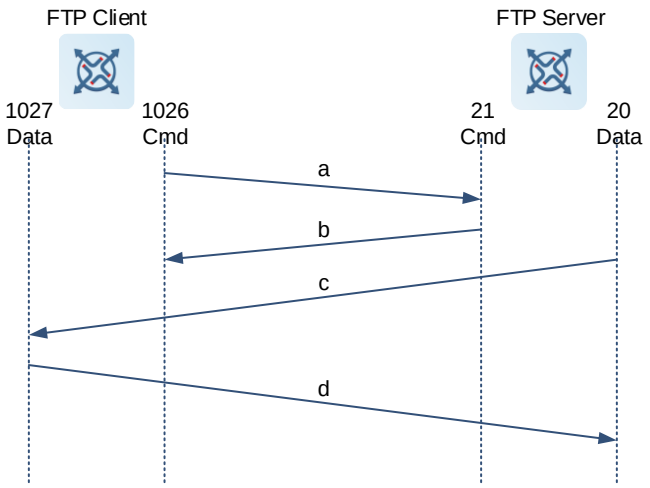
1.1.2 Principles

1. FTP Connection Mode

FTP supports two data connection modes: active (PORT) and passive (PASV). The two modes differ only in the way that a data connection is established, and the control connection is the same.

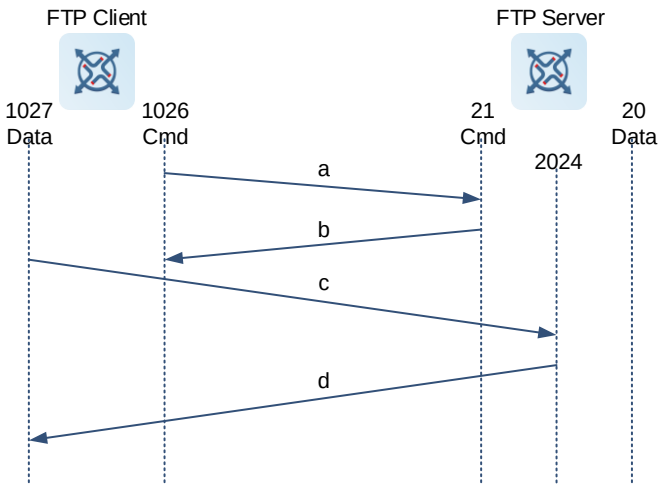
- In PORT mode, when a data connection is established, the FTP server initiates a request to establish a new connection with the client for data transmission. This mode cannot be used if the firewall is deployed on the FTP client. The connection establishment process is as follows:
  - a The FTP client establishes a control channel through port 1026 and port 21 of the FTP server, and sends control commands through this channel.
  - b The client sends the **PORT** command through this channel when it needs to receive data. The **PORT** command contains the port information (1027) of the client data channel.
  - c When transmitting data, the server connects to port 1027 of the client through port 20 on the server to establish a data channel for data transmission and reception.
  - d The client sends a response. Data transmission ends.

Figure 1-1 PORT Mode



- In PASV mode, the FTP client initiates a request when a data connection is established. The connection establishment process is as follows:
  - a The FTP client establishes a control channel through port 1026 and port 21 of the FTP server, and sends control commands through this channel.
  - b The client sends the **PASV** command through this channel when it needs to receive data.
  - c After receiving the **PASV** command, the FTP server randomly opens a high-end port 2024 and notifies the client of data transmission to this port.
  - d The client uses port 1027 to connect to port 2024 of the FTP server, and then sends or receives data on this channel. The FTP server does not need to establish a new connection with the client.

Figure 1-2 PASV Mode



Note

The control connection for command and feedback transmission is always present whereas the data connection is established as required. Only the FTP client can select the PASV or PORT mode. The FTP mode supported by an FTP client depends on the actual FTP client software. A Ruijie FTP client uses the PASV mode by default.

2. FTP File Transmission Modes

FTP provides two file transmission modes:

- Binary transmission mode: It is used to transfer program files (for example, .app, .bin and .btm files), executable files, compressed files, image files, and all ASCII values. In this transmission mode, data is not processed, and therefore the transmission rate is faster than that of the text transmission mode.
- Text transmission mode (ASCII mode): It is used to transfer text files (such as .txt, .bat, and .cfg files). This mode is different from the binary mode in carriage return and line feed processing. In ASCII mode, carriage return and line feed are converted to local CRC characters. For example, \n in Unix is \r\n in Windows or \r in Mac. Assume that a file copied by a user contains ASCII text. If a remote computer does not run Unix, FTP automatically converts the file format accepted by the remote computer during file transfer.

3. Specifying the Source IP Address for FTP Transmission

You can configure a source IP address for the FTP client and use it to communicate with an FTP server. With this IP address, the FTP client can connect to the server and share files with the server.

4. Checking Sizes of Files Downloaded from an FTP Server

When the FTP client downloads a file, it checks the file size by default to detect file transfer errors (if any). You can also disable the file size check when downloading files from FTP servers that cannot reply to FTP clients with file sizes.

1.1.3 Protocols and Standards

- RFC959: FILE TRANSFER PROTOCOL (FTP)

1.2 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring basic functions of the FTP client
  - Enabling the FTP Client to Upload Files
  - Enabling the FTP Client to Download Files
- Configuring extended functions of the FTP client
  - Configuring the FTP Connection Mode
  - Configuring the Transmission Mode of the FTP Client
  - Configuring the Source IP Address for FTP Connection

1.3 Enabling the FTP Client to Upload Files

1.3.1 Overview

You can use the FTP client to upload files to the FTP server.

1.3.2 Restrictions and Guidelines

During file transfer, do not insert or remove a storage medium or transmission medium to or from the device to avoid transmission errors.

1.3.3 Prerequisites

The user must have an account with the read and write permissions for the FTP server, and can use this account to access the target folder on the FTP server.

1.3.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Upload files.

copy flash: [*local-directory***/**] *local-file* { **ftp: | oob_ftp:** } ***//****username***:***password@destination-ip-address* [***/****remote-directory*] ***/****remote-file*

The directory specified by *local-directory* must be already configured on the device. This command does not automatically create a directory.

1.4 Enabling the FTP Client to Download Files

1.4.1 Overview

You can use the FTP client to download files from the FTP server.

1.4.2 Restrictions and Guidelines

During file transfer, do not insert or remove a storage medium or transmission medium to or from the device to avoid transmission errors.

1.4.3 Prerequisites

The user must have an account with the read permission for the FTP server, and can use this account to access the target files on the FTP server.

1.4.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Download files.

copy { **ftp: | oob_ftp:** } ***//****username***:***password@destination-ip-address* [***/****remote-directory*] ***/****remote-file* **flash:** [*local-directory***/**] *local-file*

The directory specified by *local-directory* must be already configured on the device. This command does not automatically create a directory.

(4) (Optional) Disable the size check of files downloaded from the FTP server.

ftp-client disable-size-check

By default, the sizes of files downloaded from the FTP server are checked.

1.5 Configuring the FTP Connection Mode

1.5.1 Overview

You can download or upload files in the specified FTP connection mode. The default FTP connection mode is PASV. You can set the FTP connection mode to PORT, in which the FTP server initiates a connection request to the client.

1.5.2 Restrictions and Guidelines

If you need to specify the **vrf** *vrf-name* parameter when configuring the FTP client, configure the VRF first. For details about the VRF, see "Configuring VRF" in *IP Routing*.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the connection mode to **PORT**.

ftp-client [**vrf** *vrf-name*] **port**

The default FTP connection mode is PASV.

1.6 Configuring the Transmission Mode of the FTP Client

1.6.1 Overview

You can download or upload files in the specified transmission mode of the FTP client. The default transmission mode is Binary. You can also set the transmission mode to ASCII according to your requirements.

1.6.2 Restrictions and Guidelines

If you need to specify the **vrf** *vrf-name* parameter when configuring the FTP client, configure the VRF first. For details about the VRF, see "Configuring VRF" in *IP Routing*.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the transmission mode to ASCII.

ftp-client [**vrf** *vrf-name*] **asci**

The default transmission mode is Binary.

1.7 Configuring the Source IP Address for FTP Connection

1.7.1 Overview

You can download or upload files using the specified IP address of the FTP client. The FTP client is bound to the IP address of a port so that the client can use this IP address to connect to the server.

1.7.2 Restrictions and Guidelines

If you need to specify the **vrf** *vrf-name* parameter when configuring the FTP client, configure the VRF first. For details about the VRF, see "Configuring VRF" in *IP Routing*.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the source IP address for FTP connection.

ftp-client [**vrf** *vrf-name*] **source** { *ipv4-address* | *ipv6-address* | *interface-type interface-number* }

By default, no source IP address is bound to the FTP client. Instead, an IP address is selected for the client based on the route.

1.8 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
show ftp-client	Displays the FTP client configurations.
debug ftp-client	Debugs the FTP client.

1.9 Configuration Examples

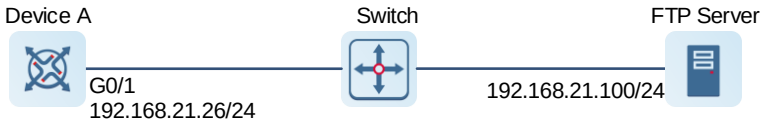
1.9.1 Configuring the FTP Client

1. Requirements

As shown in Figure 1-3, in a LAN, a local device needs to share files with a remote FTP server, and FTP is required to work in the specified connection mode and transmission mode.

2. Topology

Figure 1-3 Configuring the FTP Client



3. Notes

- Set the FTP connection mode to PORT.
- Set the transmission mode to ASCII.
- Use the username **user** and password **pass** to log in to the FTP server, upload the **local-file** file in the **home** directory of the local device to the **root** directory of the FTP server, and rename the file **remote-file**.
- Use the username **user** and password **pass** to log in to the FTP server, download the **remote-file** file from the **root** directory of the FTP server to the **home** directory of the local device, and rename this file **local-file**.

4. Procedure

(1) Configure the FTP server.

Set the IP address of the FTP server to 192.168.21.100/24.

(2) Configure device A.

a. Configure the IP address of device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.21.26 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

b. Set the transmission mode to ASCII.

```
DeviceA(config)# ftp-client ascii
```

c. Set the FTP connection mode to PORT.

```
DeviceA(config)# ftp-client port
DeviceA(config)# exit
```

d. Upload the file.

```
DeviceA# copy flash: home/local-file
ftp://user:pass@192.168.21.100/root/remote-file
```

e. Download the file.

```
DeviceA# copy ftp://user:pass@192.168.21.100/root/remote-file flash:
home/local-file
```

5. Verification

Run the **show ftp-client** command to view the FTP client configurations.

```
DeviceA> enable
DeviceA# show ftp-client
      ftp-client information
==================================
type: ASCII
mode: PORT
```

Check whether the **remote-file** file is configured on the FTP server.

Run the **dir** command to check whether the **remote-file** file is configured in the **home** directory of the Flash.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 ip address 192.168.21.26 255.255.255
!
 ftp-client ascii
 ftp-client port
!
```

7. Common Errors

- The command formats for uploading and downloading are incorrect.
- The username or password is incorrect.

Contents

1 Configuring the TFTP Server 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.1.3 Protocols and Standards 3

1.2 Configuring Basic Functions of the TFTP Server 3

1.2.1 Overview 3

1.2.2 Procedure 3

1.3 Monitoring 4

1.4 Configuration Examples 4

1.4.1 Configuring the TFTP Server 4

1 Configuring the TFTP Server

1.1 Introduction

1.1.1 Overview

Trivial File Transfer Protocol (TFTP) is a standard application layer protocol formulated by the IETF Network Working Group. TFTP uses User Datagram Protocol (UDP) as its transport protocol, and the well known UDP port for TFTP traffic is 69.

TFTP provides the uncomplicated and inexpensive file transfer service. Many commonly used FTP features are unavailable in TFTP. TFTP can only upload or download files, but not list directories, perform authentication, or provide a security mechanism. TFTP employs a timeout and retransmission strategy to ensure data transmission. TFTP is described in RFC1350.

A TFTP client can conveniently download files (such as upgrade packages) on the device from the TFTP server, or upload files directly to the file system of the TFTP server.

1.1.2 Principles

1. TFTP Packet

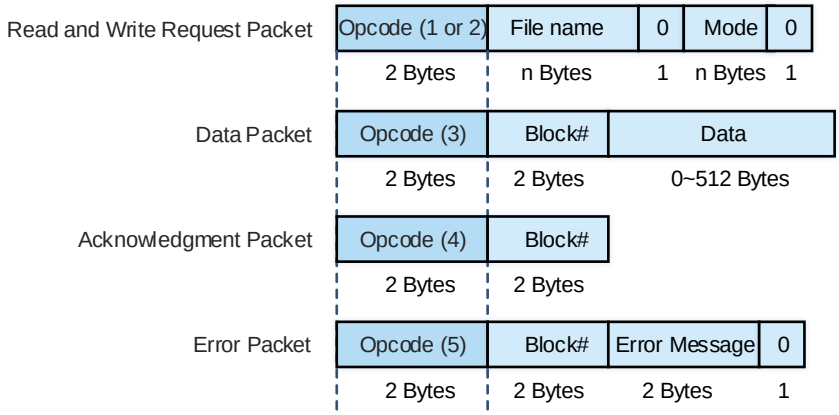
After the TFTP client initiates a file read or write request, and the TFTP server approves the request, TFTP transmits the data in 512-byte packets. A packet with less than 512 bytes indicates that the transmission is completed.

Each packet contains a data block, and the next packet can be sent only after an acknowledgment (ACK) packet is received from the peer. If the ACK packet is not received within the specified time, the last packet sent is retransmitted.

The header of a TFTP packet contains an Opcode field, which indicates the packet type. Opcodes 1 to 5 represent five types of packets:

- 1: Read Request (RRQ)
- 2: Write Request (WRQ)
- 3: Data (DATA)
- 4: Acknowledgment (ACK)
- 5: Error (ERROR)

Figure 1-1 TFTP Packet

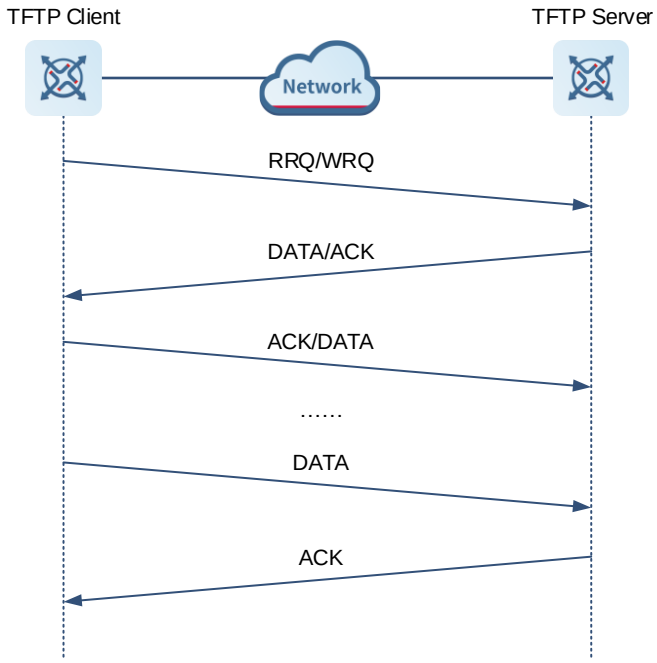


The Error Message in an error packet contains 2 bytes in ASCII code. TFTP provides the following error codes:

- 0: Not defined;
- 1: File not found;
- 2: Access violation;
- 3: Disk full;
- 4: Illegal TFTP operation;
- 5: Unknown port;
- 6: File already exists;
- 7: No such user.

2. TFTP Working Modes

Figure 1-2 TFTP Working Modes



(1) The TFTP client initiates a read request (RRQ) or write request (WRQ) to the TFTP server.

(2) If the TFTP server receives an RRQ, it checks whether the read conditions are met (whether the file exists and whether the TFTP client has the access permission). If yes, the TFTP server sends a data packet (DATA) to the TFTP client. If the TFTP server receives a WRQ, it checks whether the write conditions are met (whether there is enough space and whether the FTP client has the write permission). If yes, the TFTP server sends an ACK packet to the TFTP client.

(3) If the TFTP client receives a DATA packet when preparing to download a file, it replies with an ACK packet. If the TFTP client receives an ACK packet when preparing to upload a file, it continues to send the DATA packet.

(4) The process of sending the ACK packet repeats until the last DATA packet with less than 512 bytes is received and indicates the end of the transmission.

(5) If an error is encountered in the transmission process, an ERROR packet is sent to the peer.

3. TFTP File Transmission Modes

TFTP supports the following transmission modes:

- Binary mode for transmitting program files
- ASCII mode for transmitting text files

1.1.3 Protocols and Standards

- RFC1350: The TFTP Protocol (revision 2)
- RFC2347: TFTP Option Extension
- RFC2348: TFTP Blocksize Option
- RFC2349: TFTP Timeout Interval and Transfer Size Options

1.2 Configuring Basic Functions of the TFTP Server

1.2.1 Overview

This section describes how to configure the TFTP server to provide the upload and download service for the TFTP client.

1.2.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the top-level directory of the TFTP server.

tftp-server topdir *directory*

By default, the TFTP client can read and write files in the Flash directory.

(4) Enable the TFTP server function.

tftp-server enable

The TFTP server is disabled by default. After the TFTP server is enabled, files can be transmitted only through the MGMT port.

1.3 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
show tftp-server	Displays the TFTP server configurations.
show tftp-server updating-list	Displays the file download progress on the client.
debug tftp-server	Debugs the server.

1.4 Configuration Examples

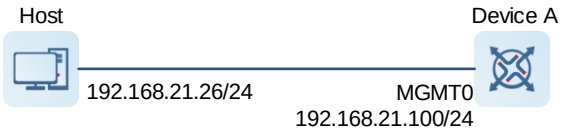
1.4.1 Configuring the TFTP Server

1. Requirements

Configure a TFTP server in a LAN so that users can upload and download files.

2. Topology

Figure 1-3 Configuring the TFTP Server



3. Notes

Configure device A as follows:

(1) Enable the TFTP server.

(2) Configure the top-level directory.

4. Procedure

(1) Configure device A.

Configure the IP address of the MGMT interface.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface mgmt 0
DeviceA(config-if-MGMT 0)# ip address 192.168.21.100 255.255.255.0
DeviceA(config-if-MGMT 0)# exit
```

Configure the top-level directory of the TFTP server.

```
DeviceA(config)# tftp-server topdir /tmp
```

Enable the FTP server function.

```
DeviceA(config)# tftp-server enable
```

(2) Configure the host.

Set the IP address of the host to 192.168.21.26/24.

5. Verification

Run the **show tftp-server** command to view the FTP server configurations.

```
DeviceA# show tftp-server
   tftp-server information
===================================
enable : Y
topdir : /tmp
```

6. Configuration Files

TFTP server configuration file

```
hostname DeviceA
!
interface MGMT 0
ip address 192.168.21.100 255.255.255.0
!
tftp-server enable
tftp-server topdir /tmp
!
```

7. Common Errors

- No top-level directory is configured.

Contents

1 Configuring TFTP Client 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 1
1.2 Configuration Task Summary 1
1.3 Enabling the TFTP Client to Upload Files 1
1.3.1 Overview 1
1.3.2 Restrictions and Guidelines 1
1.3.3 Procedure 1
1.4 Enabling the TFTP Client to Download Files 2
1.4.1 Overview 2
1.4.2 Restrictions and Guidelines 2
1.4.3 Procedure 2
1.5 Binding the Source IP Address to the TFTP Client 2
1.5.1 Overview 2
1.5.2 Procedure 2
1.6 Monitoring 3
1.7 Configuration Examples 3
1.7.1 Configuring the TFTP Client 3

1 Configuring TFTP Client

1.1 Introduction

1.1.1 Overview

Trivial File Transfer Protocol (TFTP) is a specific application of Transmission Control Protocol/Internet Protocol (TCP/IP). File transfer between TFTP client and server is implemented based on User Datagram Protocol (UDP), and the default port number is **69**. Compared with the TCP-based FTP protocol, TFTP does not require authentication or have complex packets. It is suitable for a stable network environment and small file transfer.

Note

TFTP is suitable for small file transfer, and FTP supports transfer of large files.

1.1.2 Principles

You can configure a source IP address for the TFTP client and use it to communicate with a TFTP server. With this IP address, the TFTP client can connect to the server and share files with the server. Specifying the egress interface of packets facilitates interface management.

1.1.3 Protocols and Standards

- RFC783: Trivial FILE TRANSFER PROTOCOL (TFTP)

1.2 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

- Enabling the TFTP Client to Upload Files
- Enabling the TFTP Client to Download Files
- Binding the Source IP Address to the TFTP Client

1.3 Enabling the TFTP Client to Upload Files

1.3.1 Overview

You can upload files from the TFTP client to the TFTP server.

1.3.2 Restrictions and Guidelines

During file transfer, do not insert or remove a storage medium or transmission medium to or from the device to avoid transmission errors.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Upload files.

copy flash:[*local-directory***/**] *local-file* { **tftp: | oob_tftp:** } ***//****destination-ip-address* [***/****remote-directory*] ***/****remote-file*

1.4 Enabling the TFTP Client to Download Files

1.4.1 Overview

You can download files from the TFTP server to the TFTP client.

1.4.2 Restrictions and Guidelines

During file transfer, do not insert or remove a storage medium or transmission medium to or from the device to avoid transmission errors.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Download files.

copy { **tftp:** | **oob_tftp:** } ***//****destination-ip-address* [***/****remote-directory*] ***/****remote-file* **flash:** [*local-directory***/**] *local-file*

The directory specified by *local-directory* must be already configured on the device. This command does not automatically create a directory.

1.5 Binding the Source IP Address to the TFTP Client

1.5.1 Overview

You can bind a source IP address to the TFTP client so that the client can use this IP address to communicate with the server for file upload or download.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Bind a source IP address to the TFTP client.

tftp-client source { **ip** *ipv4-address* | **ipv6** *ipv6-address* | interface-type interface-number }

By default, no source IP address is bound to the TFTP client. Instead, an IP address is selected for the client based on the route.

1.6 Monitoring

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
debug tftp	Debugs the TFTP client.

1.7 Configuration Examples

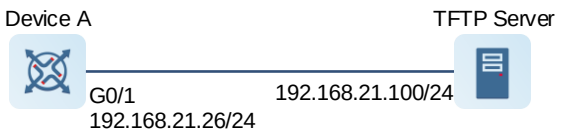
1.7.1 Configuring the TFTP Client

1. Requirements

A local device needs to upload a file to a remote TFTP server, and download another file from the TFTP server.

2. Topology

Figure 1-1 Configuring the TFTP Client



3. Notes

- Upload the **local-file** file in the **Flash** directory on device A to the **root** directory of the TFTP server with an IP address 192.168.21.100, and rename the file **remote-file**.
- Download the **remote-file** file from the **root** directory of the TFTP server with the IP address 192.168.21.100 to the **Flash** directory on device A, and save the file as **local-file**.

4. Procedure

(1) Configure the TFTP server.

Set the IP address of the TFTP Server to 192.168.21.100/24.

(2) Configure device A.

a. Configure an IP address.

```
DeviceA> enable
DeviceA# configure terminal
```

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.21.26 255.255.255
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

b. Upload the file.

```
DeviceA# copy flash:local-file tftp://192.168.23.69/root/remote-file
```

c. Download the file.

```
DeviceA# copy tftp://192.168.23.69/root/remote-file flash:local-file
```

5. Verification

Check whether the **remote-file** file is configured on the TFTP server.

Run the **dir** command on device A to check whether the **local-file** file is configured in the **home** directory of the Flash.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 ip address 192.168.21.26 255.255.255.0
!
```

7. Common Errors

- The format of the uploaded or downloaded file is incorrect.

Contents

1 Configuring SNMP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 SNMP Versions 1
1.1.3 Principles 1
1.1.4 Protocols and Standards 6
1.2 Configuration Task Summary 6
1.3 Configuring Basic SNMP Features 7
1.3.1 Overview 7
1.3.2 Restrictions and Guidelines 7
1.3.3 Procedure 7
1.4 Configuring the Trap Function 8
1.4.1 Overview 8
1.4.2 Restrictions and Guidelines 9
1.4.3 Procedure 9
1.5 Configuring the Agent Shielding Function 10
1.5.1 Overview 10
1.5.2 Restrictions and Guidelines 10
1.5.3 Procedure 10
1.6 Configuring SNMP Control Parameters 11
1.6.1 Overview 11
1.6.2 Restrictions and Guidelines 11

1.6.3 Procedure..... 11

1.7 Monitoring 12

1.8 Configuration Examples..... 13

1.8.1 Configuring Basic SNMPv2c Function..... 13

1.8.2 Configuring Basic SNMPv3 Function 14

1.8.3 Configuring Basic Trap Function..... 17

1 Configuring SNMP

1.1 Introduction

1.1.1 Overview

The Simple Network Management Protocol (SNMP) is used for network monitoring and management. Because many vendors support SNMP, SNMP has become a network management standard and applies to the interconnected environment of systems of multiple vendors. By using SNMP, the network administrator can implement information query for network nodes, network configuration, fault locating, and capacity planning.

1.1.2 SNMP Versions

- SNMPv1

  SNMPv1 is the first official version of SNMP and is defined in RFC1157. Based on community names, SNMPv1 has simple structure of management information (SMI) and simple management information base (MIB) and lower security.

- SNMPv2C

  SNMPv2 is a community-based SNMP management architecture and is defined in RFC1901. SNMPv2 is compatible with SNMPv1. Compared with SNMPv1, SNMPv2 has two more protocol operations Get-Bulk and Inform and supports more data types and error code information.

- SNMPv3

  SNMPv3 defines security extension capability and provides the following security features by identifying and encrypting data.

  - Ensuring that data is not tampered during transmission.
  - Ensuring that data is transmitted from legal data sources.
  - Encrypting packets and ensuring data confidentiality.

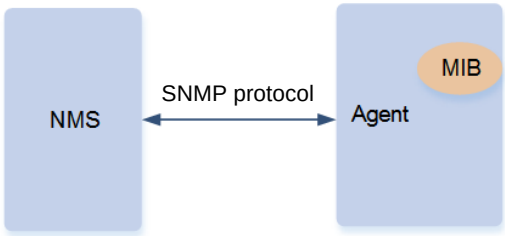
1.1.3 Principles

1. Basic Concepts

The SNMP management system has the following components:

- SNMP network manager
- SNMP agent
- MIB

Figure 1-1 Relationship Between the NMS and Network Management Agent



- SNMP network manager

  The SNMP network manager is a system that controls and monitors the network based on SNMP and is also called the network management system (NMS).

- SNMP agent

  The SNMP agent (" agent") is software running on the managed devices. It is responsible for receiving, processing, and responding to monitoring and control packets from the NMS. The agent may also actively send messages to the NMS.

- MIB

  The MIB is a virtual network management information base. The managed network devices contain lots of information. To uniquely identify a specific management unit among SNMP packets, the MIB adopts the tree hierarchical structure. Nodes in the tree indicate specific management units. A string of digits are used to uniquely identify a management unit system among network devices. The MIB is a set of unit identifiers of network devices.

- Operation types

  Six operation types are defined for information exchange between the NMS and the agent based on SNMP:

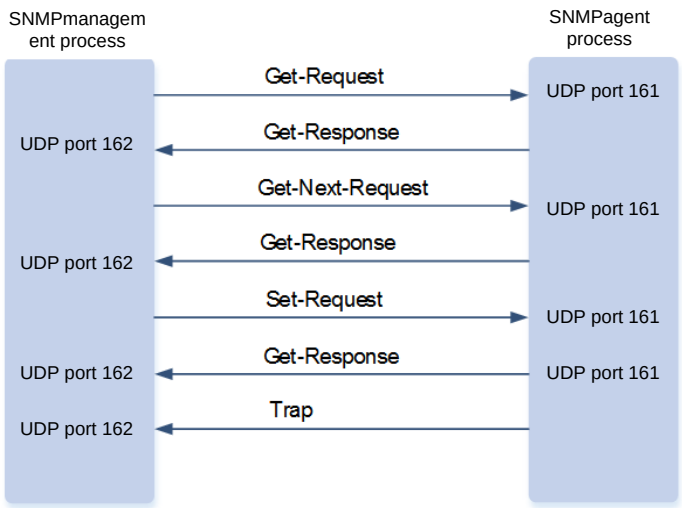
  - Get-Request: The NMS extracts one or more parameter values from the agent.
  - Get-Next-Request: The NMS extracts the parameter value next to one or more parameters from the agent.
  - Get-Bulk: The NMS extracts a batch of parameter values from the agent.
  - Set-Request: The NMS sets one or more parameter values of the agent.
  - Get-Response: The agent returns one or more parameter values, which are the operations of the agent in response to the three operations performed by the NMS.
  - Trap: The agent actively sends a message to notify the NMS of something that happens.

  The first four packets are sent by the NMS to the agent and the last two packets are sent by the agent to the NMS. The first three operations of the NMS and the response operations of the agent are based on UDP port 161. The Trap operation performed by the agent is based on UDP port 162. For details, see Figure 1-2.

Caution

SNMPv1 does not support the Get-Bulk operation.

Figure 1-2 SNMP Packet Interaction



2. Basic SNMP Functions

SNMP interaction is response interaction (for interaction of packets, see Figure 1-2). The NMS actively sends requests to the agent, including Get-request, Get-next-request, Get-bulk, and Set-request. The agent receives the requests, completes operations, and returns a Get-response. Sometimes, the agent actively sends a Trap message and an Inform message to the NMS. The NMS does not need to respond to the Trap message but needs to return an Inform-response to the agent. Otherwise, the agent re-sends the Inform message.

3. Principles of SNMPv1 and SNMPv2C

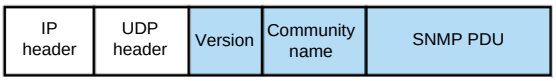
SNMPv1 and SNMPv2C adopt the community-based security architecture. The administrator who can perform operations on the MIB of the agent is limited by defining the host address and authentication name (community string).

SNMPv1 and SNMPv2 determine whether the administrator has the right to use MIB objects by using the authentication name. To be able to manage devices, the NMS must ensure that its authentication name is the same as an authentication name defined in devices.

In SNMPv2C, the Get-bulk operation enables more detailed error message types to be returned to the NMS. The Get-bulk operation allows all information from a table or lots of data to be obtained at a time, so as to reduce the request-response times. The enhanced error handling capabilities of SNMPv2C include extension of error codes to differentiate error types. In SNMPv1, however, only one error code is provided for the errors. In SNMPv2C, the error codes can be used to differentiate error types. Because management workstations on the network may support SNMPv1 and SNMPv2C at the same time, the SNMP agent must be able to identify SNMPv1 packets and SNMPv2C packets and return packets of the corresponding versions.

SNMPv1 and SNMPv2c packets are composed of version, community name, and SNMP protocol data unit (PDU). Figure 1-3 shows the structure of the packets.

Figure 1-3 Structure of SNMPv1 and SNMPv2c Packets



- The main fields in packets are as follows:
  - Version: Indicates an SNMP version. For SNMPv1 packets, the corresponding field value is 0. For SNMPv2c packets, the field value is 1.
  - Community name: It is used for authentication between the agent and NMS. The field value is a string that can be customized. The community names include readable and writable community names. During Get-Request and Get-Next-Request operations, a readable community name is used for authentication. During Set operations, a writable community name is used for authentication.
  - SNMP PDU: Includes information such as PDU type, request identifier, and variable binding list. SNMPv1 PDUs include GetRequest PDU, GetNextRequest PDU, SetRequest PDU, Response PDU, and Trap PDU. Compared with SNMPv1, SNMPv2c has GetBulkRequest PDU and InformRequest PDU.
- Security

  An authentication name has the following attributes:
  - Read-only: Provides the read permission of all MIB variables for authorized management workstations.
  - Read-write: Provides the read/write permission of all MIB variables for authorized management workstations.

4. Principles of SNMPv3

SNMPv3 redefines the SNMP architecture and includes functions of SNMPv1 and SNMPv2 into the SNMPv3 system.

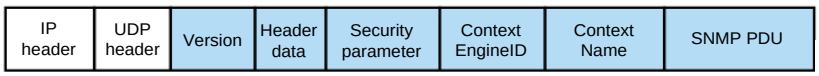
The NMS and SNMP agent are SNMP entities. In the SNMPv3 architecture, SNMP entities consist of the SNMP engine and SNMP applications. The SNMP engine is used to send and receive messages, identify and encrypt information, and control access to managed objects. SNMP applications refer to internal applications of SNMP, which work by using the services provided by the SNMP engine.

SNMPv3v determines whether a user has the right to use MIB objects by using the user-based security model (USM). The security level of the NMS user must be the same as that of an SNMP user defined in devices so as to manage devices.

SNMPv3 requires the NMS to obtain the SNMP agent engine IDs on devices when the NMS manages devices. SNMPv3 defines the Discover and Report operation mechanisms. When the NMS does not know the agent engine ID, the NMS may first send a Discover message to the agent and the agent returns a Report message carrying an engine ID. Later, management operations between the NMS and the agent must carry the engine ID.

SNMPv3 defines a new packet format, which is shown in Figure 1-4.

Figure 1-4 Structure of SNMPv3 Packets



- The main fields in SNMP packets are as follows:
  - Version: Indicates an SNMP version. For SNMPv3 packets, the field value is 2.

- Header data: Mainly includes description information such as the maximum message size supported by the message sender and the security model of the message.
- Security parameter: Includes such security information as SNMP engine-related information, username, authentication parameter, and encryption parameter.
- Context EngineID: A unique identifier of SNMP. This field and the PDU type decide the application to which the packets are sent.
- Context name: Decides the MIB view of the managed devices based on the Context EngineID.
- SNMP PDU: Includes information such as PDU type, request identifier, and variable binding list. SNMPv3 PDUs include GetRequest PDU, GetNextRequest PDU, SetRequest PDU, Response PDU, Trap PDU, GetBulkRequest PDU, and InformRequest PDU.

- Security

  SNMPv3 determines the data security mechanism based on the security model and security level. At present, security models include SNMPv1, SNMPv2C, and SNMPv3. SNMPv3 includes SNMPv1 and SNMPv2C into the security model.

Table 1-1 Security Models and Security Levels of SNMPv1 and SNMPv2C

Security Model	Security Level	Authentication	Encryption
SNMPv1	noAuthNoPriv	Authentication name	N/A
SNMPv2c	noAuthNoPriv	Authentication name	N/A

Table 1-2 Security Model and Security Level of SNMPv3

Security Model	Security Level	Authentication	Encryption	Description
SNMPv3	noAuthNoPriv	Username	N/A	Data validity is confirmed through username.
SNMPv3	authNoPriv	MD5 or SHA	N/A	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA is provided.
SNMPv3	authPriv	MD5 or SHA	DES	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA and the data encryption mechanism based on CBC-DES are provided.

- Engine ID

  An engine ID is used to uniquely identify an SNMP engine. Because each SNMP entity includes only one SNMP engine, the SNMP engine uniquely identifies an SNMP entity in a management domain. Therefore, the SNMPv3 agent as an entity must has a unique engine ID, that is, SnmpEngineID.

  An engine ID is an octet string that consists of 5 to 32 bytes. RFC3411 defines the format of an engine ID:

  - The first four bytes indicate the private enterprise ID (allocated by the Internet Assigned Numbers Authority (IANA)) of a vendor, which is expressed in hexadecimal.

- The fifth byte indicates remaining bytes.
- 0: Reserved.
- 1: The later four bytes indicate an IPv4 address.
- 2: The later 16 bytes indicate an IPv6 address.
- 3: The later six bytes indicate a MAC address.
- 4: Text consisting of up to 27 bytes, which is defined by the vendor.
- 5: Hexadecimal value consisting of up to 27 bytes, which is defined by the vendor.
- 6-127: Reserved.
- 128-255: Formats specified by the vendor.

1.1.4 Protocols and Standards

- RFC 1157, Simple Network Management Protocol (SNMP)
- RFC 1901, Introduction to Community-based SNMPv2
- RFC 2578, Structure of Management Information Version 2 (SMIv2)
- RFC 2579, Textual Conventions for SMIv2
- RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413, Simple Network Management Protocol (SNMP) Applications
- RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
- RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP)
- RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

RFC 3419, Textual Conventions for Transport Addresses

1.2 Configuration Task Summary

SNMP configuration includes the following tasks:

(1) Configuring Basic SNMP Features

(2) (Optional) Configuring the Trap Function

(3) (Optional) Configuring the Agent Shielding Function

(4) (Optional) Configuring SNMP Control Parameters

1.3 Configuring Basic SNMP Features

1.3.1 Overview

After the basic SNMP function is configured, users can access the agent through the NMS.

1.3.2 Restrictions and Guidelines

- When an authentication name is configured, the default access permission is read-only if no access permission is specified.
- When the view-based access control model (VACM) is used, an SNMP user group must be configured. By associating users with a group and associating the group with a view, you can ensure that the users in the group have the same access permission. In this way, you can determine whether managed objects associated with an operation are in the allowable range of a view. Only managed objects in the range of a view can be accessed.
- When you configure users in SNMPv3, you can specify the security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (DES at present), and encryption password.
- After the SNMP attack prevention and detection function is configured, the corresponding action can be taken after authentication fails consecutively.
- The permanently forbidden source IP addresses can be authenticated for access again only after the administrator manually unlocks the IP addresses. The source IP addresses that are forbidden in a period of time can be authenticated for access again after the period expires or after the administrator manually unlocks the IP addresses.
- By default, password dictionary check is not performed for communities and users. If community names and usernames are too simple and are easily cracked, enable password dictionary check for the communities and users. The configuration must be used with the **password policy** command in the global configuration mode.
- The SNMP logging function records the Get, Get-Next, and Set operations performed by the NMS on the SNMP Agent. When the Get and Get-Next operations are performed, the agent records the IP address of the NMS user, operation type, and OID of the operation node. When the Set operation is performed, the agent records the IP address of the NMS user, operation type, OID of the operation node, and set value. These logs are sent to the information center of devices. The level of these logs is informational, that is, the logs are used as prompt information of devices. A large number of logs will affect device performance. In normal conditions, you are advised to disable the SNMP logging function.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure an SNMP view.

snmp-server view *view-name oid-tree* { **include** | **exclude** }

An SNMP view needs to be configured when the View-based Access Control Model (VACM) function is used.

The default view allows access to all MIB objects.

(4) (Optional) Configure an SNMP user group.

snmp-server group *group-name* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { [**ipv6** *ipv6-acl-name*] *acl-name* | *acl-number* }]

No user group is configured by default.

(5) Configure an authentication name and access permission.

snmp-server community [**0** | **7** | **secret** [**0** | **8**]] *community-string* [**view** *view-name*] [**ro** | **rw**] [**host** *ipv4-address* | **host** *ipv6-address*] [**ipv6** *ipv6-acl-name*] [*acl-name* | *acl-number*]

No authentication name is configured and the access permission of all communities is read-only by default.

When SNMPv1 and SNMPv2C are used to manage network devices, an authentication name must be configured on the agent.

(6) Configure an SNMP user.

snmp-server user *username groupname* { **v1** | **v2c** | **v3** [**encrypted** | **interactive**] [**auth** { **md5** | **sha** | **sha2-256** | **sha2-512** } *auth-password*] [**priv** { **des56 | acs128** } *priv-password*] } [**access** { [**ipv6** *ipv6-acl-name*] *acl-name* | *acl-number* }]

No SNMP user is configured by default.

When SNMPv3 is used to manage network devices, a user must be configured.

(7) (Optional) Enable the agent function.

enable service snmp-agent

The SNMP agent function is enabled by default.

(8) (Optional) Enable the SNMP attack prevention and detection function.

snmp-server authentication attempt *attempt-times* **exceed** { **lock** | **lock-time** *lock-time* | **unlock** }

The SNMP attack prevention and detection function is disabled by default.

(9) (Optional) Configure password dictionary check for communities and users.

snmp-server enable secret-dictionary-check

Password dictionary check is not configured for communities and users by default.

(10) (Optional) Configure the SNMP logging function to record the Get, Get-Next, and Set Operations performed by the NMS on the SNMP Agent.

snmp-server logging { **get-operation** | **set-operation** | **trap-info** }

By default, the SNMP logging function is disabled.

1.4 Configuring the Trap Function

1.4.1 Overview

After the Trap function is configured, the agent actively sends Trap messages to the NMS.

1.4.2 Restrictions and Guidelines

- The host address of the NMS must be configured when the agent actively sends Trap messages to the NMS. That is, the **snmp-server host** command is used with the **snmp-server enable traps** command in the global configuration mode.
- Multiple SNMP hosts can be configured to receive Trap messages. A host can combine different types of Trap messages, ports, and VRF forwarding tables. If a host is configured with the same port and VRF in multiple configurations, the last configuration is combined with the previous configurations. To send different Trap messages to the same host, configure different types of Trap messages each time. These configurations are finally combined.
- The system reboot notification function must be enabled on the agent so that the RGOS system sends Trap messages to the NMS to notify system reboot before reloading or rebooting of the device.
- After the Link Trap message sending function is enabled on an interface, the SNMP sends a Link Trap message if the link status on the interface changes. Otherwise, the SNMP does not send the message.
- By default, the IP address of an interface that sends SNMP packets is used as the source address of the SNMP packets. If you want to use a fixed local IP address as the source address to facilitate management, configure the source address for sending Trap messages on the agent.
- The **snmp-server trap-format private** command can be run to include private fields in Trap messages. The supported private field is the alarm generation time. For the specific data types and data ranges of the fields, see the RUIJIE-TRAP-FORMAT-MIB.mib file.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure an NMS host address.

snmp-server host [**oob**] { *ipv4-addrress* | **ipv6** *ipv6-address* | **domain** *domain-name* } [**vrf** *vrf-name*] [**informs** | **traps**] [**version** { { **1** | **2c** } [**0** | **7**] *community* | **3** { **auth** | **noauth** | **priv** } *username* }] [**udp-port** *port-number*] [**via** *mgmt-name*] [*notification-type*] No SNMP host address is configured by default.

(4) (Optional) Enable the agent to actively send Trap messages to the NMS.

snmp-server enable traps [*notification-type*]

The SNMP agent is forbidden to send Trap messages to the NMS by default.

(5) (Optional) Enable the Link Trap message sending function on an interface.

snmp-server link-status

The Link Trap message sending function is enabled on an interface by default.

(6) (Optional) Configure the system reboot trap sending function.

snmp-server system-shutdown

The SNMP system reboot notification function is disabled by default.

(7) (Optional) Configure a source address for Trap messages.

snmp-server trap-source *interface-type interface-number*

The IP address of the interface that sends SNMP packets is used as the source address by default.

(8) (Optional) Include private fields in sent Trap messages.

snmp-server trap-format private

SNMP Trap messages do not include private fields by default.

(9) Configure Inform message sending attempts and timeout time.

snmp-server inform { **retries** *retry-number* | **timeout** *timeout* }

The number of default Inform message sending attempts is **3** and the default Inform message timeout time is **15** seconds.

1.5 Configuring the Agent Shielding Function

1.5.1 Overview

After the agent shielding function is enabled, the port access frequency and network attack probability are reduced.

1.5.2 Restrictions and Guidelines

The SNMP agent function is disabled by default. When SNMP agent parameters (for example, NMS host address, authentication name, and access permission) are configured, the SNMP agent service is automatically enabled. The **enable service snmp-agent** command must be run so that the SNMP agent service can take effect. If the SNMP agent service is disabled or the **enable service snmp-agent** command is not run, the SNMP agent service does not take effect. The **no snmp-server** command is used to shield all SNMP agent service configurations. In this case, running the **show running-config** command will not display the configurations. The configurations can be restored after the SNMP agent service is enabled again. The **no enable service snmp-agent** command is used to disable the SNMP agent service. In this case, the SNMP agent function is disabled and packets and trap messages are not sent and received, but the SNMP agent configurations are not shielded.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the SNMP agent shielding function.

no snmp-server

The SNMP agent function is enabled by default.

(4) Disable the SNMP agent function of a device.

no enable service snmp-agent

The SNMP agent function is enabled by default.

1.6 Configuring SNMP Control Parameters

1.6.1 Overview

After basic parameters such as device contact mode, device location, serial number, and Trap message sending are configured, the NMS can obtain information such as the contact person and physical location of the device by accessing the parameters.

1.6.2 Restrictions and Guidelines

- When too many SNMP request packets cause SUMP tasks to occupy a large CPU space, you can configure SNMP traffic control to limit the number of request packets processed per second in each SNMP task to control the CPU usage.
- SNMP contains three versions: v1, v2C, and v3. If only a specified version is used for MIB interaction management in a user scenario, you can disable unused SNMP versions by running the **no snmp-server enable version** [**v1** | **v2c** | **v3**] command.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the contact mode of the system.

snmp-server contact *contact-text*

The contact mode of the system is empty by default.

(4) Configure the system location.

snmp-server location *location-text*

The system location is empty by default.

(5) Configure the system serial number.

snmp-server chassis-id *chassis-id-text*

The default system serial number is 60FF60.

In general, the device serial number is used as the SNMP serial number to facilitate identification of the device.

(6) Configure NE information of a device.

snmp-server net-id *net-id-text*

The NE code information of a device is empty by default.

(7) Configure the maximum packet length of the SNMP agent.

snmp-server packetsize *packetsize*

The maximum packet length of the SNMP agent is 1,472 bytes by default.

(8) Configure the UDP port ID of the SNMP service.

snmp-server udp-port *port-number*

The default UDP port ID of the SNMP service is **161**.

(9) Configure the source port of the device on which the SNMP service is deployed.

snmp-server source-interface *interface-type interface-number*

The source port of a device with a valid IP address is used to receive SNMP packets by default.

(10) Configure the queue length of Trap messages.

snmp-server queue-length *queue-length*

The default queue length of the Trap messages is **100**.

(11) Configure the sending interval of Trap messages.

snmp-server trap-timeout *trap-timeout-time*

The Trap messages are resent with a timeout time of **300** milliseconds by default.

(12) Configure SNMP traffic control.

snmp-server flow-control pps *packet-count*

About 300 SNMP request packets are processed every second by default.

(13) Configure the status of SNMP versions.

no snmp-server enable version [**v1** | **v2c** | **v3**]

All SNMP versions are enabled by default.

1.7 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Caution

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

Table 1-3 Monitoring

Command	Purpose
clear snmp locked-ip [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]	Clears the list of source IP addresses that are locked after authentication fails consecutively.
show snmp [**group** | **host** | **locked-ip** | **process-mib-time** | **mib** | **user** | **version** | **view**]	Displays the SNMP status information.

1.8 Configuration Examples

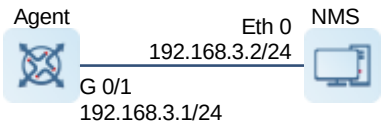
1.8.1 Configuring Basic SNMPv2c Function

1. Requirements

Network devices are managed and monitored through the SNMP network manager, as shown in Figure 1-5.

2. Topology

Figure 1-5 Topology of Basic SNMPv2 Function



3. Procedure

Enable the SNMP agent function.

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# enable service snmp-agent
```

Configure a read/write community with the name comm_v1.

```
Ruijie(config)# snmp-server community comm_v2 rw
```

Configure an IP address for the agent. Set the address of GigabitEthernet 0/1 to 192.168.3.1/24.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)# ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)# exit
```

4. Verification

Run the **ping** command to verify that the agent and NMS are mutually reachable via L3 routes.

```
Ruijie# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **show service** command to check whether the SNMP agent function is enabled.

```
Ruijie# show service
snmp-agent    : enabled
ssh-server    : disabled
telnet-server : enabled
```

5. Configuration Files

Agent configuration file

```
interface GigabitEthernet 0/1
```

```
 ip address 192.168.2.1 255.255.255.0
!
snmp-server community comm_v2 rw
!
end
```

1.8.2 Configuring Basic SNMPv3 Function

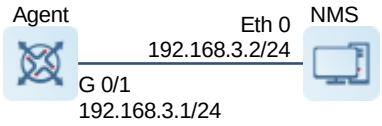
1. Requirements

The network management station is connected to the managed network devices. On the network management station, users access the MIB on the network devices through the SNMP network manager and receive messages actively sent by the network devices to manage and monitor the network devices.

- The management workstation (NMS) manages network devices (agents) based on the authentication and encryption mode of users.
- Network devices can control the operation permission of users to access MIB objects.
- Network devices can actively send authentication and encryption messages to the NMS.

2. Topology

Figure 1-6 Topology of Basic SNMPv3 Function



3. Notes

- Configure an MIB view and an SNMP user group.
- Configure an SNMP user.
- Configure an SNMP host.
- Configure an IP address for the agent.

4. Procedure

Create an MIB view with the name view1, which includes the associated MIB object 1.3.6.1.2.1.1. Create an MIB view with the name view2, which includes the associated MIB object 1.3.6.1.2.1.1.4.0.

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# snmp-server view view1 1.3.6.1.2.1.1 include
```

Create an MIB view with the name view2, which includes the associated MIB object 1.3.6.1.2.1.1.4.0.

```
Ruijie(config)# snmp-server view view2 1.3.6.1.2.1.1.4.0 include
```

Create an SNMP user group with the name g1, select v3 as the version, and configure an authentication and encryption mode with the security level priv. Configure view1 as a readable view and view2 as a writable view.

```
Ruijie(config)# snmp-server group g1 v3 priv read view1 write view2
```

Configure an SNMP user. Create a user with the name **user1** under the group g1, select v3 as the version, and set the authentication mode to md5, authentication password to 123, encryption mode to DES56, and encryption password to 321.

```
Ruijie(config)# snmp-server user user1 g1 v3 auth md5 123 priv des56 321
```

Configure the SNMP host: Set the host address to 192.168.3.2, and the version to v3, configure an authentication and encryption mode with the security level priv, and associate the username **user1**.

```
Ruijie(config)# snmp-server host 192.168.3.2 traps version 3 priv user1
```

Enable the agent to actively send Trap messages to the NMS.

```
Ruijie(config)# snmp-server enable traps
```

Configure an IP address for the agent. Set the address of GigabitEthernet 0/1 to 192.168.3.1/24.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)# ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)# exit
```

5. Verification

Run the **ping** command to verify that the agent and NMS are mutually reachable via L3 routes.

```
Ruijie# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **show snmp user** command to display the SNMP user.

```
Ruijie# show snmp user
User name: user1
Engine ID: 800013110300d0f8221120
storage-type: permanent    active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: g1
```

Run the **show snmp view** command to display the SNMP view.

```
Ruijie# show snmp view
view1(include) 1.3.6.1.2.1.1
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1.3.6.1
```

Run the **show snmp group** command to display the SNMP group.

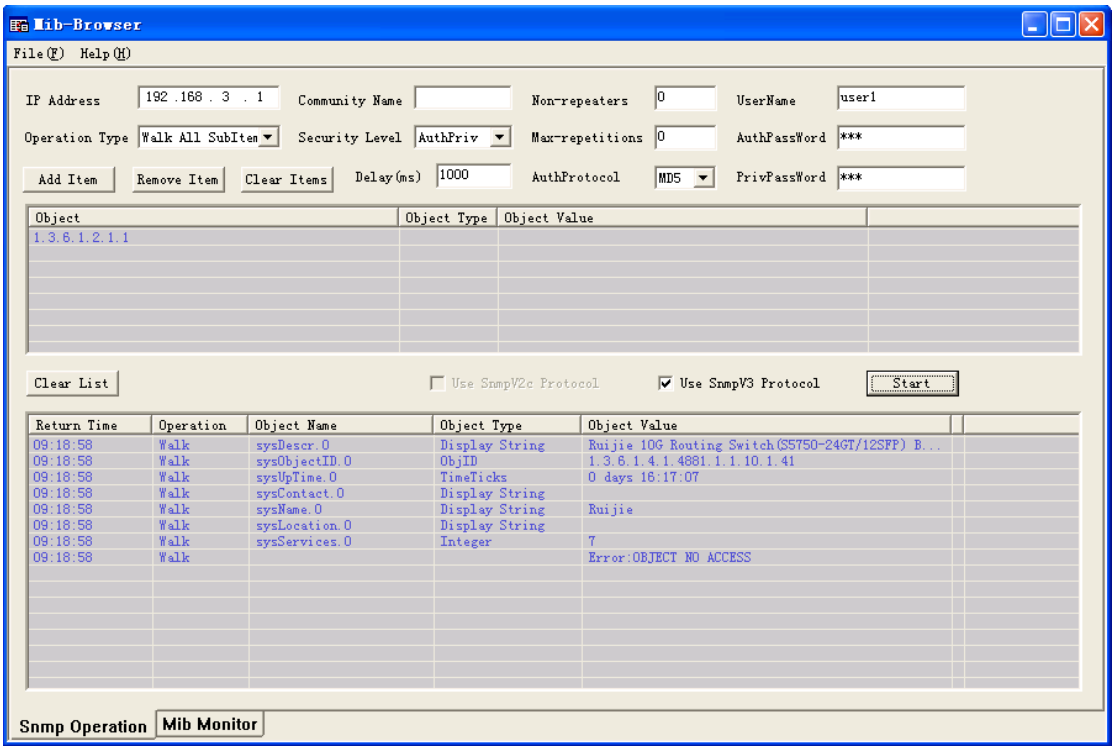
```
Ruijie# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: view1
writeview: view2
notifyview:
```

Run the **show snmp host** command to display the host information configured by the user.

```
Ruijie# show snmp host
Notification host: 192.168.3.2
udp-port: 162
type: trap
user: user1
security model: v3 authPriv
```

Install the MIB browser query. Enter the IP address 192.168.3.1 in IP Address and **user1** in UserName, select AuthPriv for Security Level, enter 123 in AuthPassWord, select MD5 for AuthProtocol, and enter 321 in PrivPassWord. Click **Add Item** and select an MIB management unit to be queried, for example, System. Click **Start** to query the MIB of the network devices. The query results are displayed in the lowest pane of the dialog box, as shown in Figure 1-7.

Figure 1-7 MIB-browser Query Example



6. Configuration Files

Agent configuration file

```
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
!
snmp-server view view1 1.3.6.1.2.1.1 include
snmp-server view view2 1.3.6.1.2.1.1.4.0 include
snmp-server user user1 g1 v3 encrypted auth md5 DE8E9D1158A057A69EF73D1C12C51CC5 priv
des56 C767B705F9B261E6D359D4BFBDAF9CF4
snmp-server group g1 v3 priv read view1 write view2
snmp-server host 192.168.3.2 traps version 3 priv user1
```

```
snmp-server enable traps
!
end
```

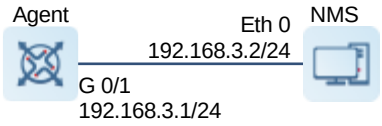
1.8.3 Configuring Basic Trap Function

1. Requirements

The network management station (NMS) manages network devices (agents) based on the community authentication mode, and the network devices can actively send messages to the network management station.

2. Topology

Figure 1-8 Topology of Basic Trap Function



3. Procedure

Set the agent and NMS to be reachable via L3 routes, and set the IP address of GigabitEthernet 0/1 on the agent to 192.168.3.1.

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

Set the SNMP host address to 192.168.3.2, the message format to Version 2c, and the authentication name to user1. Enable the agent to actively send Trap messages to the NMS.

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# snmp-server host 192.168.3.2 traps version 2c user1
Ruijie(config)# snmp-server enable traps
```

4. Verification

Run the **ping** command to verify that the agent and NMS are mutually reachable via L3 routes.

```
Ruijie# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **show snmp** command to display the SNMP status.

```
Ruijie# show snmp
Chassis: 1234567890
0 SNMP packets input
```

```
       0 Bad SNMP version errors
       0 Unknown community name
       0 Illegal operation for community name supplied
       0 Encoding errors
       0 Number of requested variables
       0 Number of altered variables
       0 Get-request PDUs
       0 Get-next PDUs
       0 Set-request PDUs
0 SNMP packets output
       0 Too big errors (Maximum packet size 1472)
       0 No such name errors
       0 Bad values errors
       0 General errors
       0 Response PDUs
       0 Trap PDUs
SNMP global trap: enabled
SNMP logging: disabled
SNMP agent: enabled
```

5. Configuration Files

Agent configuration file

```
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
!
snmp-server host 192.168.3.2 traps version 2c user1
snmp-server enable traps
!
end
```

Contents

1 Configuring RMON 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 3
1.2 Configuration Task Summary 3
1.3 Configuring the Ethernet Statistics Function 3
1.3.1 Overview 3
1.3.2 Restrictions and Guidelines 3
1.3.3 Procedure 4
1.4 Configuring the History Statistics Function 4
1.4.1 Overview 4
1.4.2 Restrictions and Guidelines 4
1.4.3 Procedure 4
1.5 Configuring the Alarm Function 5
1.5.1 Overview 5
1.5.2 Restrictions and Guidelines 5
1.5.3 Procedure 5
1.6 Monitoring 5
1.7 Configuration Examples 6
1.7.1 Configuring the Ethernet Statistics Function 6
1.7.2 Configuring the History Statistics Function 7

1.7.3 Configuring the Alarm Function 10

1 Configuring RMON

1.1 Introduction

1.1.1 Overview

The Remote Network Monitoring (RMON) protocol is a network management protocol that is built on the Simple Network Management Protocol (SNMP) architecture. RMON provides statistics and alarm functions for a managing device to remotely monitor and manage devices. he statistics function means that a managed device can trace and calculate different types of traffic information on a network segment that is connected to the port of the device regularly or continuously. For example, the device can trace and calculate the total number of packets or the total number of excessively long packets received on a network segment in a period. The alarm function means that a managed device can monitor specified management information base (MIB) variables and automatically record an event and send Trap messages to the managing device when one of the variables reaches the alarm threshold, for example, the port rate or the ratio of broadcast packets reaches a specified value.

Both RMON and SNMP are used for remote network management. Compared with SNMP, RMON has the following advantages:

- RMON notifies the managing device of alarm variable abnormality in Trap messages by using the SNMP Trap message sending mechanism. Though the Trap function is also defined in SNMP, this function is used to notify the managing device of the function running status of a managed device and physical state change of an interface. SNMP and RMON have different monitored objects, trigger conditions, and report content.
- Compared with SNMP, RMON can monitor remote network devices more effectively and actively, thus providing an efficient means of monitoring subnet running. According to RMON, a managed device can automatically send Trap messages when a value reaches the alarm threshold. This frees the managing device from frequently obtaining and comparing values of MIB variables and thus reduces the communication between the managing device and managed device. As a result, large interconnected networks are being managed simply yet effectively.

1.1.2 Principles

RMON defines different RMOM groups, and Ruijie devices support the statistics group, history group, alarm group, and event group. The four groups are as follows:

1. Statistics Group

A statistics group is used to monitor and calculate traffic data on an Ethernet interface. The traffic data consists of cumulative values and is calculated from the time of entry creation to the current time. Statistical objects include discarded packets, broadcast packets, CRC errors, over-small or over-large packets, and conflicts. The statistical results are saved in the Ethernet statistical table for the administrator to view at any time.

2. History Group

A history group is used to collect network traffic periodically and records cumulative values of the traffic and bandwidth usage in each period. The data is saved in the history control table for the administrator to process. A history group includes two sub-groups:

- The HistoryControl sub-group is used to configure control information such as sampling interval and sampling data sources.
- The EthernetHistory sub-group provides the administrator with history data of a specific network segment, including traffic, error packets, broadcast packets, usage, and hit times.

3. Alarm Group

The alarm group is used to monitor specified MIB objects. When the value of an MIB object exceeds the set upper limit or lower limit, an alarm is triggered and processed as an event.

4. Event Group

An event group is used to define processing methods of events. When a monitored MIB object reaches the alarm condition, an event is triggered. The event can be processed with one of the following methods:

- None: The event is ignored.
- Log: The event related information is recorded in a log table for the administrator to view at any time.
- Snmp-trap: The Trap message is sent to the network management station to notify the occurrence of the event.
- Log-and-trap: The event-related information is recorded in a log table and the Trap message is sent to the network management station.

5. Working Process of RMON

RMON allows multiple monitor authorities to collect data with the following two methods: use the special RMON probe to collect data so that the NMS can obtain all MIB information from the RMON probe; embed the RMON agent into a network device (for example, switch or router) so that the device possesses the function of an RMON probe. The NMS uses basic commands of SNMP to exchange data with the network device and collect network management information. Limited by the device resources, this method does not obtain all data of the RMON MIB. Generally, only four groups of information are collected.

Through the RMON agent running on the managed network device, the NMS can obtain information such as traffic, error statistics, and performance statistics on the network segment that is connected to the port of this network device, to remotely manage this network device. Figure 1-1 shows the communication network between the NMS and RMON agent.

- RMON Ethernet statistics function

  Make the statistics of network traffic on the Ethernet interface from the time of entry creation to the current time.

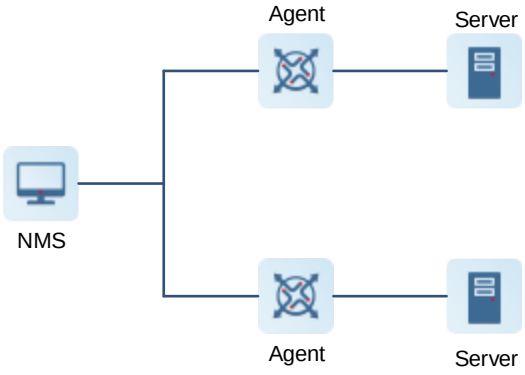
- RMON history statistics function

  Record cumulative statistical values of traffic on the Ethernet interface in each period.

- RMON alarm function

  Monitor changes of alarm variable values periodically. If an alarm variable value exceeds the specified upper or lower limit, corresponding event is triggered, for example, a Trap message is sent or a LogTable entry record is created. Continuous excess of an upper or a lower limit triggers an event only once and the event can be triggered again by excess of the opposite limit.

Figure 1-1 Communication Network Between the NMS and RMON Agent



1.1.3 Protocols and Standards

- STD 0059 / RFC 2819: Remote Network Monitoring Management Information Base
- RFC4502: Remote Network Monitoring Management Information Base Version 2
- RFC 3919: Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)
- RFC 3737: IANA Guidelines for the Registry of Remote Monitoring (RMON) MIB Modules
- RFC 3434: Remote Monitoring MIB Extensions for High Capacity Alarms
- RFC 3395: Remote Network Monitoring MIB Protocol Identifier Reference Extensions
- RFC 3287: Remote Monitoring MIB Extensions for Differentiated Services
- RFC 3273: Remote Network Monitoring Management Information Base for High Capacity Networks
- RFC 2896: Remote Network Monitoring MIB Protocol Identifier Macros
- RFC 2895: Remote Network Monitoring MIB Protocol Identifier Reference

1.2 Configuration Task Summary

RMON configuration includes the following tasks:

- Configuring the Ethernet Statistics Function
- Configuring the History Statistics Function
- Configuring the Alarm Function

1.3 Configuring the Ethernet Statistics Function

1.3.1 Overview

With the Ethernet statistics function of RMON, you can learn the cumulative statistical values of traffic generated on the monitored Ethernet interface from the time of entry creation to the current time.

1.3.2 Restrictions and Guidelines

- To calculate and monitor a specified interface, you must configure the Ethernet statistics function on this interface.

- After the statistics entry is created on the specified interface, the statistics group calculates the traffic of this interface. That is, make the statistics of variables defined by the Ethernet statistics table and record the cumulative values of variables that are generated from the creation time of the RMON statistics table to the current time.
- This function cannot be configured in the batch interface configuration mode.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure statistical items of RMON.

rmon collection stats *collection-stats-table-index* [**owner** *owner-name*]

The Ethernet statistics function is not configured on an Ethernet interface by default.

1.4 Configuring the History Statistics Function

1.4.1 Overview

With the history statistics function of RMON, you can learn the cumulative statistical values of traffic generated in each period and the bandwidth utilization on the monitored interface.

1.4.2 Restrictions and Guidelines

- The history group makes the statistics of variables defined by the history statistics function and records cumulative values of variables in each period.
- To collect network statistics on a specified interface, you must configure the history control function on the interface. This function cannot be configured in the batch interface configuration mode.
- It is not allowed to modify parameters of the configured history statistics function.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

Interface *interface type interface number*

(4) Configure the history statistics function of an Ethernet interface.

rmon collection history *collection-history-table-index* [**buckets** *bucket-number*] [**interval** *period-time*] [**owner** *owner-name*]

The history statistics function is not configured on an Ethernet interface by default.

1.5 Configuring the Alarm Function

1.5.1 Overview

The alarm function of RMON monitors whether the values of alarm variables vary within the valid range periodically.

1.5.2 Restrictions and Guidelines

- If alarm variables are MIB variables defined by the RMON statistical group or history group, the RMON statistics function or history statistics function must be configured on the monitored Ethernet interface. Otherwise, the alarm table fails to be created.
- The alarm function is implemented by the alarm table and event table. After an alarm event is triggered, the SNMP agent must be configured so that Trap messages can be sent to the managing device. For more information about SNMP agent configuration, see "Configuring SNMP" in *NMS and Monitoring Configuration Guide*.
- Configured event table parameters, including event type, Trap community name, event description, and event creator, can be modified.
- Configured alarm table parameters, including alarm variable, sampling type, table creator, sampling interval, upper/lower limit, and event, can be modified.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an event table.

rmon event *event-table-index* [**description** *description-string*] [**log**] [**owner** *owner-name*] [**trap** *community*]

No RMON event is configured by default.

(4) Configure the alarm function.

rmon alarm *alarm-table-index alarm-variable sampling-interval* { **absolute** | **delta** } **rising-threshold** *ampling-rising-threshold-value* [*event-number*] **falling-threshold** *falling-threshold*-[*event-number*] [**owner** *owner-name*]

The RMON alarm function is not configured by default.

1.6 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show rmon	Displays all RMON configurations.
show rmon stats	Displays the Ethernet statistics table information.
show rmon history	Displays the history control table information.
show rmon alarm	Displays the alarm table information.
show rmon event	Displays the event table information

1.7 Configuration Examples

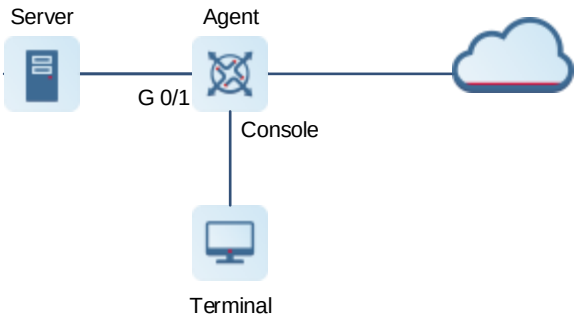
1.7.1 Configuring the Ethernet Statistics Function

1. Requirements

The RMON agent is connected to a server. The network administrator uses the RMON statistics group to calculate the performance of received packets on GigabitEthernet 0/1. Thus, the network administrator can understand the data of packets received on an interface at any time by viewing data, and take timely actions to process network abnormalities.

2. Topology

Figure 1-2 Topology of the RMON Ethernet Statistics Function



3. Procedure

Configure a statistics table instance on GigabitEthernet 0/1 of the device on which the RMON agent is deployed to make the statistics of traffic on this interface.

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# rmon collection stats 1 owner admin
```

4. Verification

Run the **show rmon stats** command to display Ethernet statistics information.

```
Ruijie# show rmon stats
ether statistic table:
                index = 1
                interface = GigabitEthernet 0/1
                owner = admin
                status = 1
                dropEvents = 0
                octets = 25696
                pkts = 293
                broadcastPkts = 3
                multiPkts = 0
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                packets64Octets = 3815
                packets65To127Octets = 1695
                packets128To255Octets = 365
                packets256To511Octets = 2542
                packets512To1023Octets = 152
                packets1024To1518Octets = 685
```

5. Configuration Files

Agent configuration file

```
hostname Ruijie
!
interface GigabitEthernet 0/1
 rmon collection stats 1 owner admin
!
end
```

6. Common Errors

The parameters of configured statistics entries are reconfigured or modified.

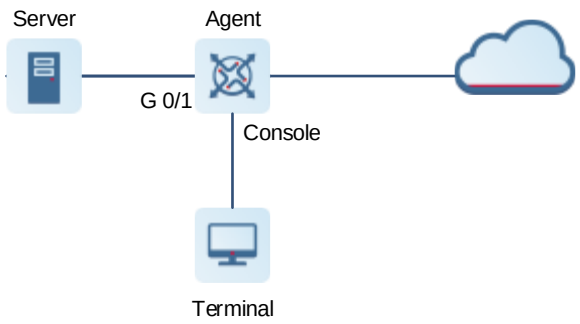
1.7.2 Configuring the History Statistics Function

1. Requirements

The RMON agent is connected to a server. The network administrator uses the history group to make the statistics of received packets on GigabitEthernet 0/1 every minute so as to monitor the network and master emergencies.

2. Topology

Figure 1-3 Topology of the History Statistics Function



3. Procedure

Configure a history control table on GigabitEthernet 0/1 of the device on which the RMON agent is deployed to make the statistics of traffic on this interface periodically.

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# rmon collection history 1 buckets 5 interval
300 owner admin
```

4. Verification

Run the **show rmon history** command to display history group statistics.

```
Ruijie# show rmon history
rmon history control table:
                index = 1
                interface = GigabitEthernet 0/1
                bucketsRequested = 5
                bucketsGranted = 5
                interval = 60
                owner = admin
                stats = 1

rmon history table:
                index = 1
                sampleIndex = 786
                intervalStart = 6d:18h:37m:38s
                dropEvents = 0
                octets = 2040
                pkts = 13
                broadcastPkts = 0
                multiPkts = 0
                crcAlignErrors = 0
```

```
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0

                index = 1
                sampleIndex = 787
                intervalStart = 6d:18h:38m:38s
                dropEvents = 0
                octets = 1791
                pkts = 16
                broadcastPkts = 1
                multiPkts = 0
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0

                index = 1
                sampleIndex = 788
                intervalStart = 6d:18h:39m:38s
                dropEvents = 0
                octets = 432
                pkts = 6
                broadcastPkts = 0
                multiPkts = 0
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0

                index = 1
                sampleIndex = 789
                intervalStart = 6d:18h:40m:38s
                dropEvents = 0
                octets = 432
                pkts = 6
                broadcastPkts = 0
```

```
                multiPkts = 0
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0

                index = 1
                sampleIndex = 790
                intervalStart = 6d:18h:41m:38s
                dropEvents = 0
                octets = 86734
                pkts = 934
                broadcastPkts = 32
                multiPkts = 23
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0
```

5. Configuration Files

Agent configuration file

```
hostname Ruijie
!
interface GigabitEthernet 0/1
 rmon collection history 1 buckets 5 interval 300 owner admin
!
end
```

6. Common Errors

The parameters of configured history control entries are reconfigured or modified.

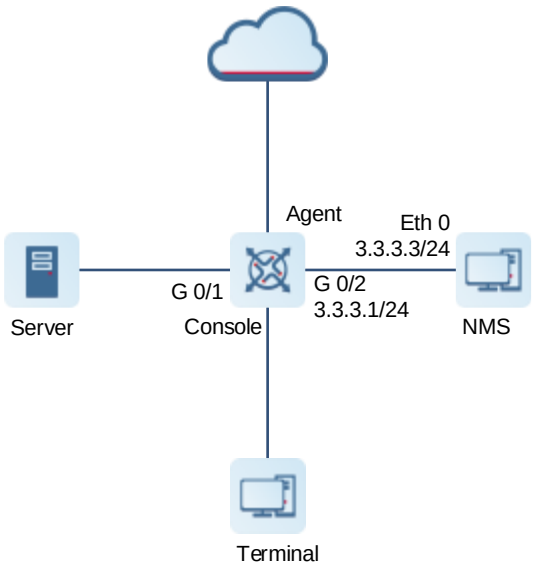
1.7.3 Configuring the Alarm Function

1. Requirements

The RMON agent is configured on a terminal device and connected to the NMS device for communication. The port GigabitEthernet 0/1 is connected to the server and must be monitored the number of received packets with unknown protocols. The sampling interval is 60 seconds. When the absolute collection value is smaller than 10, only a log record is generated. When the absolute sampling value is greater than 100, a log record is generated and a notification is sent to the NMS in a Trap message.

2. Topology

Figure 1-4 Topology of the Alarm Function



3. Notes

- Run SNMPv1 on the NMS, configure a community name public1, set the attribute to RW, and set the Trap message receiving address to 3.3.3.3.
- Monitor the number of packets with unknown protocols, received on GigabitEthernet0/1, and check whether the OID value is 1.3.6.1.2.1.2.2.1.15.3, sampling method is relative sampling, and sampling interval is 60 seconds. Check whether event 1 or event 2 is triggered when the relative sampling value is greater than 100 or smaller than 10. For event 1, a Trap message is sent and a log record is generated. For event 2, a log record is generated.

4. Procedure

Set the IP address of GigabitEthernet0/2 on the agent to 3.3.3.1.

```
Ruijie> enabel
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 3.3.3.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# exit
```

Configure an event group to process alarms.

```
Ruijie(config)# snmp-server community public1 rw
Ruijie(config)# snmp-server host 3.3.3.3 trap public1
Ruijie(config)# rmon event 1 description rising-threshold-event log trap public owner
admin
Ruijie(config)# rmon event 2 description falling-threshold-event log owner admin
```

Configure the alarm function.

```
Ruijie(config)# rmon alarm 1 1.3.6.1.2.1.2.2.1.15.3 60 delta rising-threshold 100 1
falling-threshold 10 2 owner admin
```

5. Verification

Run the **ping** command to verify that the agent and NMS are mutually reachable via L3 routes.

```
Ruijie# ping 3.3.3.3
Sending 5, 100-byte ICMP Echoes to 3.3.3.3, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms.
```

Run the **show rmon event** command to display the event table information.

```
Ruijie# show rmon event
rmon event table:
                index = 1
                description = rising-threshold-event
                type = 4
                community = public
                lastTimeSent = 0d:0h:0m:0s
                owner = admin
                status = 1

                index = 2
                description = falling-threshold-event
                type = 2
                community =
                lastTimeSent = 6d:19h:21m:48s
                owner = admin
                status = 1

rmon log table:
                eventIndex = 2
                index = 1
                logTime = 6d:19h:21m:48s
                logDescription = falling-threshold-event
```

Run the **show rmon alarm** command to display the alarm table information.

```
Ruijie# show rmon alarm
rmon alarm table:
         index: 1,
         interval: 60,
         oid = 1.3.6.1.2.1.2.2.1.15.3
         sampleType: 2,
         alarmValue: 0,
         startupAlarm: 3,
         risingThreshold: 100,
         fallingThreshold: 10,
```

```
        risingEventIndex: 1,
        fallingEventIndex: 2,
        owner: admin,
        stauts: 1
```

6. Configuration Files

Agent configuration file

```
hostname Ruijie
!
interface GigabitEthernet 0/1
 ip address 3.3.3.1 255.255.255.0
!
rmon alarm 1 1.3.6.1.2.1.2.2.1.15.3 60 delta rising-threshold 100 1 falling-threshold
10 2 owner admin
rmon event 1 description rising-threshold-event log trap public1 owner admin
rmon event 2 description falling-threshold-event log owner admin
!
snmp-server host 3.3.3.3 traps public1
snmp-server community public1 rw
!
end
```

7. Common Errors

- The entered object OID is improper. For example, the variable corresponding to this OID does not exist or the OID type is not an integer or unsigned integer.
- The upper limit is smaller than or equal to the lower limit.

Contents

1 Configuring CWMP 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.1.3 Protocols and Standards 6

1.2 Configuration Task Summary 6

1.3 Configuring CWMP 6

1.3.1 Establishing a Basic CWMP Connection 6

1.3.2 Configuring CWMP Attributes 8

1.4 Monitoring 9

1.5 Configuration Examples 9

1.5.1 Configuring Basic CWMP Functions 9

1 Configuring CWMP

1.1 Introduction

1.1.1 Overview

The CPE WAN Management Protocol (CWMP), also known as TR-069 protocol, is a management protocol initiated and developed by Digital Subscriber's Line (DSL) forum and numbered TR-069. CWMP provides a general framework of unified device management, related message specifications, management methods, and data models. It solves difficulties in unified management and maintenance of dispersed customer premises equipment (CPEs), improves troubleshooting efficiency, and saves O&M costs.

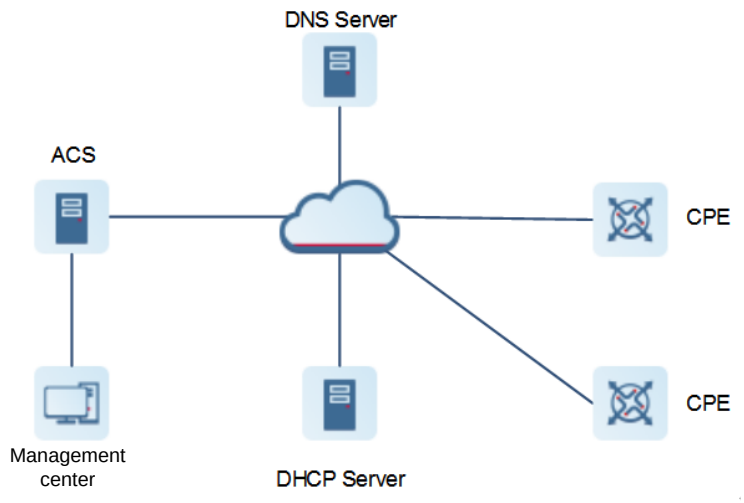
1.1.2 Principles

1. Basic Concepts

Figure 1-1 shows the network structure of CWMP, mainly including:

- ACS: The auto-configuration server (ACS) is the managing device in a network.
- CPE: The customer premises equipment (CPE) is the managed device in a network.
- DHCP server: The Dynamic Host Configuration Protocol (DHCP) server obtains the Uniform Resource Locator (URL) of the ACS dynamically.
- DNS server: The dynamic network server (DNS) parses domain names of the ACS or CPE.

Figure 1-1 Network Structure of CWMP



2. Network Structure of CWMP

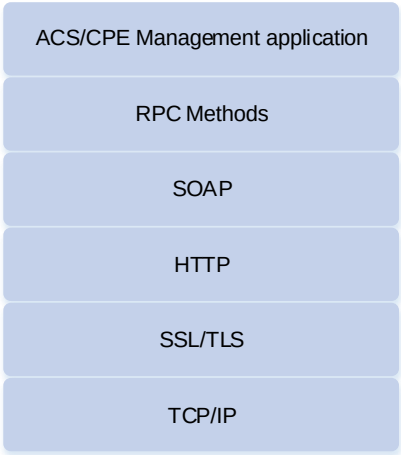
As shown in Figure 1-2, CWMP work is composed of six layers:

- ACS/CPE management application: This layer is not a part of CWMP. It is the development performed by functional modules of the CPE/ACS to support CWMP. As with the Simple Network Management Protocol (SNMP), CWMP does not cover the management information base (MIB) management of functional

modules.

- RPC methods: This layer provides and implements various RPC methods for interactions between the ACS and the CPE. The ACS manages and monitors the CPE with mostly the following RPC methods:
- Get series methods: The Get methods enable the ACS to remotely obtain RPC methods, as well as names, values and attributes of the data model parameters supported on the CPE.
- Set series methods: The Set methods enable the ACS to remotely set the values and attributes of the data model parameters supported on the CPE.
- Inform method: The Inform method enables the CPE to inform the ACS of their device identifiers, parameter information, and events. This is the first method used when sessions are established between the ACS and the CPE.
- Download method: The Download method enables the ACS to remotely control and manage file download of the CPE, including main program upgrade, configuration file upgrade, and Web package upgrade.
- Upload method: The Upload method enables the ACS to remotely control and manage file upload of the CPE, including configuration file and log file upload.
- Reboot method: The Reboot method enables the ACS to remotely control reboot of the CPE.
- SOAP: The Simple Object Access Protocol (SOAP) layer uses an XML-based syntax to encode and decode CWMP messages. Thus, CWMP messages must comply with the XML-based syntax of SOAP.
- HTTP: The Hypertext Transfer Protocol (HTTP) layer transmits all CWMP messages. Both the ACS and the CPE can behave in the role of HTTP clients and servers. The server is used to monitor reverse connections from the peer.
- SSL/TLS: The secure sockets layer (SSL) or transport layer security (TLS) layer guarantees CWMP security, including data integrity, confidentiality, and authentication.
- TCP/IP: This layer is the Transmission Control Protocol/Internet Protocol (TCP/IP) stack.

Figure 1-2 CWMP Structure



3. Working Process of CWMP

Figure 1-3 shows the working process of CMWP.

(1) Create a TCP connection.

(1) Create a security mechanism during SSL initialization.

(2) After the CPE sends an Inform packet, start establishing a CWMP connection. Use the Eventcode field to describe the cause of sending this Inform packet in the Inform packet.

(3) If the CPE passes the ACS authentication, the ACS returns an Inform response packet to establish the connection.

(4) If the CPE has no more request, a null packet is sent to meet the rule of HTTP request/response packet interaction. CWMP is based on HTTP, and CWMP packets as data parts of HTTP packets are encapsulated in HTTP packets.

(5) The ACS queries the value of the ACS URL set on the CPE.

(6) The CPE returns the obtained ACS URL to the ACS.

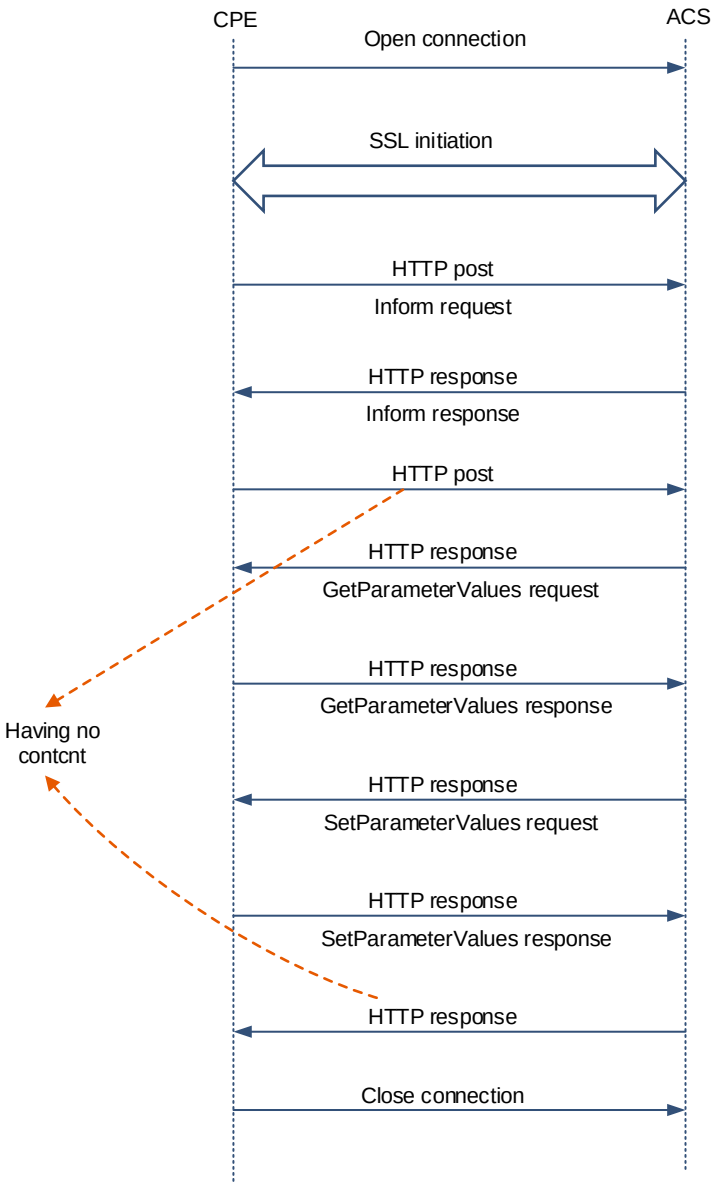
(7) When the ACS discovers that the ACS URL is not the local URL value, the ACS initiates a Set request, requesting the CPE to set its ACL URL to the URL value of the standby ACS.

(8) After the ACL URL is set, the CPE sends a response packet.

(9) The ACS sends a null packet to notify the CPE, there are any other requests.

(10) The CPE closes the session.

Figure 1-3 Work Flowchart of CWMP



- Session management

  CWMP sessions are the basis for CWMP. All CWMP interactions between the ACS and the CPE rely on the sessions. The interaction effectiveness of the sessions is ensured by the transmission, management, and maintenance for effective management and monitoring. An ACS-CPE session is a TCP connection, which starts from the Inform negotiation to TCP disconnection. Sessions are classified into those initiated by the CPE and those requested by the ACS according to the session initiator.

  - The CPE initiates a connection

    The CPE can initiate a connection with the ACS based on the configured ACS address at any time. In the following scenarios, the CPE must establish a connection with the ACS.

    When the CPE is powered on, reset or initialized, the CPE establishes a connection with the ACS for the first time.

    When the ACS URL changes,

an Inform packet must be sent if a parameter is changed.

When the CPE receives a valid connection request from the ACS,

and the CPE is configured to periodically send Inform packets, it sends connection requests both automatically and periodically.

When the CPE is configured to send Inform packets periodically, the CPE automatically send connection requests at the designated time point.

- The ACS initiates a connection

  The ACS can, at any time, require the CPE to initiate a connection request to the ACS by using the connection request notification mechanism to set up the connection with the CPE.

Note

- The CPE must support the connection request notification mechanism. If the ACS is required to actively initiate a connection request, the ACS must support the connection request notification mechanism.
- Communication at least once between the ACS and the CPE is the prerequisite for ACS to initiate a connection. If the ACS desires to actively initiate communication, the ACS stores the management IP address of the CPE in the communication. If the management IP address of the CPE changes, the CPE must send an Inform packet to notify the ACS of the new management IP address to timely update the information of the ACS.

4. Basic Functions of CWMP

CWMP provides mainly the following functions:

- Auto configuration

  After the CPE starts operation, the management center can deliver configuration to the CPE through the ACS server to change the CPE configuration and status and thus manage the CPE. The configuration file is delivered with two methods:

  - Update the configuration file. The configuration file of the CPE is replaced with a specified configuration file so that the new configuration file is run on the CPE after reset.
  - Update running configuration. Specific configuration is directly delivered to the CPE and saved to the running configuration of the CPE. The configuration takes effect immediately upon delivery. The configuration must be saved. Otherwise, the delivered configuration will be lost after CPE reset.

- Status and performance monitoring

  The CPE notifies the ACS of the current status and configuration change of the device through the periodic Inform mechanism. The ACS monitors the CPE based on these notifications of the real-time change.

- Fault diagnosis

  According to the diagnostic information provided by the CPE, the ACS resolves connection problems and other service problems and executes some predefined diagnostic actions.

- Main program upgrade

  Main program upgrade means updating main program of the CPE so as to upgrade software version of the CPE. When the ACS detects any latest version of the main program, the ACS delivers the Download method to the CPE. The CPE downloads the main program from the file server specified in the Download method. After the main program is downloaded and the CPE checks the validity of the main program, the

CPE restart to upgrade the main program. After restart, the CPE notifies the ACS of the completion of main program upgrade.

- Data backup

  The ACS controls the CPE to upload configuration files to the ACS or file server with the Upload method.

Note

The file server can be ACS or separately deployed.

- Backup and restoration

  CPE backup and restoration means that when any remote CPE breaks away from the management center due to an abnormal operation on the ACS, the CPE must be restored to the previous status, so that the ACS can correctly manage and operate the remote device of the CPE once again.

  Generally, the CPE breakaway is caused by the delivered incorrect main program or configuration. The CPE must be configured to restore the main program or configuration if any abnormality arises. When the CPE receives any main program upgrade or configuration delivery request, the CPE backs up the current configuration and main program version. After the upgrade or update is completed, the CPE determines whether it is broken away from the ACS. If yes, the CPE restores itself to the previous manageable status.

1.1.3 Protocols and Standards

- TR069: CPE WAN Management Protocol

1.2 Configuration Task Summary

CWMP configuration includes the following tasks:

(1) Establishing a Basic CWMP Connection

(2) (Optional) Configuring CWMP Attributes

1.3 Configuring CWMP

1.3.1 Establishing a Basic CWMP Connection

1. Overview

A session connection is established between the ACS and the CPE.

2. Restrictions and Guidelines

- Only one ACS username can be configured. If the ACS name is configured repeatedly, the latest username configured takes effect.
- The ACS user password can be in plaintext or cyphertext form. Only one ACS user password can be configured. If the ACS password is configured repeatedly, the latest password configured takes effect.
- Only one ACS URL can be configured. If the ACS URL is configured repeatedly, the latest URL configured takes effect. The ACS URL must be in HTTP format.
- When a CPE password is configured for authentication in the connection with the ACS, the encryption type does not need to be entered. If an encrypted password is copied and pasted, the encryption type must be

entered. A valid password should meet the following format requirements:

- Contain 1 to 26 characters including uppercase letters, lowercase letters, and digits.
- Leading spaces will be ignored, while the trailing and middle spaces are valid.

- Only one CPE URL can be configured for the connection between the CPE and the ACS. If the CPE URL is configured repeatedly, the latest URL configured takes effect. The CPE URL must be in HTTP format instead of domain name format. By default, a CPE URL is automatically selected based on the ACS URL. The CPE URL format must meet the following requirements:
  - Follow the http://ip [: port]/ format.
  - Contain 256 characters at most.
- Only one CPE username can be configured. If the CPE username is configured repeatedly, the latest user configured takes effect.
- If the ACS URL is not manually configured but a dynamic ACS URL is obtained through DHCP, this dynamic ACS URL is used to initiate a connection to the ACS. The ACS URL must meet the following format requirements:
  - Follow the format of http://ip[:port]/path.
  - Contain 256 characters at most.
- The **cpe source** command and the **cpe url** command are not compatible with each other. When the two commands are not configured, the CPE automatically selects URL based on the ACS URL.
  - The interface name of the CPE must be the full name of the interface and can be automatically filled when a CLI command is entered.
  - If no port ID is configured, the default port ID 7547 is used.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the CWMP function.

cwmp

The CWMP function is enabled by default.

(4) Configure an ACS username for CWMP connection.

acs username *username*

No ACS username is configured for CWMP connection by default.

(5) Configure an ACS password for CWMP connection

acs password { **0** *encryption-type* | **7** *encrypted-password* | *password* }

No ACS password is configured for CWMP connection by default.

(6) (Optional) Configure a CPE username for CWMP connection.

cpe username *username*

No CPE username is configured for CWMP connection by default.

(7) Configure a CPE password for CWMP connection.

cpe password { **0** *encryption-type* | **7** *encrypted-password* | *password* }

No CPE password is configured for CWMP connection by default.

(8) Configure an ACS URL for CWMP connection.

acs url *url*

No ACS URL is configured for CWMP connection by default.

(9) Configure a CPE URL for CWMP connection.

cpe url *url*

No CPE URL is configured for CWMP connection by default.

(10) Configure the CPE URL based on the IP address of the specified interface.

cpe source interface *interface-type interface-number* [**port** *port-number*]

No CPE URL is configured based on the IP address of the specified interface by default.

1.3.2 Configuring CWMP Attributes

1. Overview

You can configure common functions for CPE, for example, backup and restoration of main program and configuration file, acceptance or not of main program and configuration file delivered by the ACS, management or not of configuration/log files uploaded to the ACS.

2. Restrictions and Guidelines

- Any CPE can be configured with the periodic Inform function.
  - If no Inform start time is configured, the Inform enabling time is used as the Inform start time, and Inform is performed once every default Inform interval. For example, no Inform period or start time is configured, but the Inform function is enabled at 12:00 a.m. Then, periodic Inform will start at 12:00 a.m. next day and be performed once every default Inform interval.
  - If the Inform start time is configured, periodic Inform starts at the specified start time. For example, if the Inform interval is set to 60 seconds and the start time is 12:00 a.m. next day, periodic Inform will start at 12:00 a.m. next day and be performed once every 60 seconds.
- If you do not expect CPE to receive any main program and configuration file from the ACS, you can disable the management Inform function of receiving the main program and configuration file delivered by the ACS. Disabling the function of receiving the main program and configuration file delivered by the ACS does not act on configuration script files. The configuration scripts can still be executed even if this function is disabled.
- If you do not expect CPE to upload configuration file and log file to the ACS, you can disable the management function of uploading any configuration file and log file to the ACS.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the CWMP configuration mode.

cwmp

(4) (Optional) Configure CWMP attributes. Configure at least one of the following tasks.

- Enable the periodic Inform function on the CPE.

  cpe inform [**interval** *interval*] [**starttime** *hh:mm:ss MM/DD/YY*]

  The periodic Inform function of the CPE is disabled by default. The default Inform period is 600 seconds.

- Enable the management Inform function of receiving any main program and configuration file delivered by the ACS.

  no disable download

  The management function of receiving any main program and configuration file delivered by the ACS is enabled by default.

- Enable the management function of uploading any main program and configuration/log file to the ACS from the CPE.

  no disable upload

  The management function of uploading any main program and configuration/log file upload function to the ACS is enabled by default.

- Enable the backup and restoration function of the CPE main program or configuration file.

  cpe back-up [**delay-time** *time*]

  The backup and restoration function of the main program or configuration file is disabled by default.

- Configure the CPE timeout time in the case of no ACS response.

  timer cpe-timeout *tiemout*

  The default CPE timeout time is 30 seconds in the case of no ACS response.

1.4 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the current running status of CWMP.

1.5 Configuration Examples

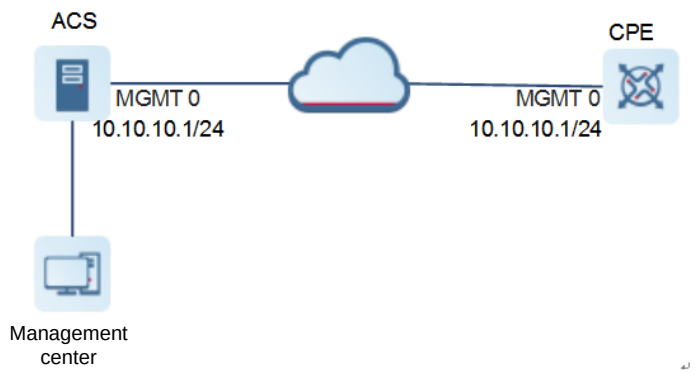
1.5.1 Configuring Basic CWMP Functions

1. Requirements

Many network devices are configured in the corporate network, as shown in Figure 1-4. The network administrator manages and monitors these devices through CWMP to improve O&M efficiency.

2. Topology

Figure 1-4 Topology of Basic CWMP Functions



3. Notes

- Configure that the CPE and ACS are mutually reachable via routes.
- Enable the CWMP function on the CPE.

4. Procedure

Configure an IP address for the network management interface of the CPE.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface mgmt 0
Hostname(config-if-Mgmt 0)# ip address 10.10.10.10 255.255.255.0
Hostname(config-if-Mgmt 0)# gateway 10.10.10.1
```

Configure a URL connection between the ACS and CPE.

```
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# acs url http://10.10.10.10:7547/acs
Hostname(config-cwmp)# cpe url http://10.10.10.1:7547/
```

Set the periodic Inform interval of the CPE to 60 seconds.

```
Hostname(config-cwmp)#cpe inform interval 60
```

Set the backup and restoration delay to 30 seconds.

```
Hostname(config-cwmp)# cpe back-up delay-time 30
```

Set the CPE timeout time to 30 seconds in the case of no ACS response.

```
Hostname(config-cwmp)# timer cpe-timeout 100
```

Disable the management function of any main program and configuration file delivered and downloaded by the ACS.

```
Hostname(config-cwmp)# disable download
```

Disable the management function of uploading any main program, configuration file and log file to the ACS.

```
Hostname(config-cwmp)# disable upload
```

Configure the username and password of the ACS.

```
Hostname(config-cwmp)# acs username USERB
Hostname(config-cwmp)# acs password PASSWORDB
```

Configure the username and password of the CPE.

```
Hostname(config-cwmp)# cpe username USERB
Hostname(config-cwmp)# cpe password PASSWORDB
```

5. Verification

Run the **ping** command to check whether the CPE and ACS are mutually reachable via L3 routes.

```
Hostname# ping oob 10.10.10.1
Sending 5, 100-byte ICMP Echoes to 10.10.10.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms.
Hostname#
```

Run the **show cwmp configuration** command to display the CWMP configuration result on the CPE.

```
Hostname# show cwmp configuration
CWMP status                  : enable
ACS URL                     : http://10.10.10.10:7547/acs
ACS username                 : USERB
ACS password                 : PASSWORDB
CPE source interface name      :
CPE URL                     : http://10.10.10.1:7547/
CPE username                 : USERB
CPE password                 : PASSWORDB
CPE inform status             : enable
CPE inform interval           : 60s
CPE inform start-time         : 0:0:0 0 0 0
CPE wait timeout             : 100s
CPE download status           : disable
CPE upload status            : disable
CPE back up status           : enable
CPE back up delay time        : 30s
CPE STUN port-adaptive        : enable
CPE STUN probe nat agingtime   : enable
CPE STUN port                : 3478
CPE STUN max-period           : 60s
CPE STUN min-period           : 20s
```

6. Configuration Files

Device A configuration file

```
hostname Hostname
!
cwmp
```

```
 acs url http://10.10.10.10:7547/acs
 acs username USERB
 acs password PASSWORDB
 cpe source interface GigabitEthernet 0/1
 cpe username USERB
 cpe password PASSWORDB
 timer cpe-timeout 100
 disable upload
 cpe back-up delay-time 30

!
interface Mgmt 0
 ip address 10.10.10.10 255.255.255.0
 gateway 10.10.10.1
```

7. Common Errors

- The entered password is cyphertext and the password length exceeds 254 or the password is not an even number.
- The entered password is plaintext and longer than 126 characters.
- The entered password is plaintext and contains illegal characters.
- The ACS URL is null.
- The CPE URL is null.

Contents

1 Configuring SEM 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Basic Concepts 1
1.1.3 Principle 3
1.2 Configuration Task Summary 4
1.3 Enabling the SEM Function 5
1.3.1 Overview 5
1.3.2 Restrictions and Guidelines 5
1.3.3 Configuring SEM Policies 5
1.3.4 Configuring Parameters of SEM Policies 7
1.4 Monitoring 8
1.5 Configuration Examples 9
1.5.1 Configuring an Interface Monitoring Event 9
1.5.2 Configuring a Counter Monitoring Event 11
1.5.3 Configuring a Syslog Monitoring Event 15
1.5.4 Configuring a Track Monitoring Event 18

1 Configuring SEM

1.1 Introduction

1.1.1 Overview

The smart embedded manager (SEM) is a network management tool. It is embedded in a device and can be separately deployed. The tool supports command configuration, independent from external network management tools, which makes the tool easier to deploy.

Traditional external network management tools must be connected to devices over a network to manage the devices. If a network fails, affecting network connection, the external network management tools lose effect. SEM can directly manage devices under any circumstance and troubleshoot different types of network or device faults or capture key information.

SEM detects user configuration events in real time. When an event occurs, SEM takes preset actions. The entire procedure is highly customizable. SEM provides fault detection and processing and automatic management functions, which improves the availability of the device and network.

SEM supports a variety of events, including key events of a device such as key syslog, trap and time point, or user input operations such as Command Line Interface (CLI) commands and Simple Network Management Protocol (SNMP) operations, or threshold excess such as interface statistics, SNMP object values, and system resource statistics. SEM supports many actions, including user command running, log sending, and active device reset.

1.1.2 Basic Concepts

- Event

  An event indicates an event that a user cares about. It is configured by users and attached to a policy. One or multiple events can be configured. Each type of events are detected by a specific detector. When conditions are met, corresponding event is triggered by the event detector. For example, to detect the inclusion of the **shutdown** command in the privileged EXEC mode, run the **event tag** *example* **cli pattern** *shutdown* **mode** *exec* command to configure this event to the corresponding command line event detector.

- Action

  An action indicates a measure taken after an event occurs. It is configured by users and attached to a policy. One or multiple actions can be configured. Each type of actions correspond to a type of action configurations. When an event occurs, the policy corresponding to this event runs configured actions in order. For example, to restart a device after an event occurs, run the **action** *example* **reload** command.

- Policy

  A policy organizes relationships between events and between events and actions. A policy must be submitted after it is configured. When an event corresponding to this policy meets a preset rule, this policy is triggered and runs actions in order.

- Event detector

An event detector is embedded in specific business and monitors the business based on user configuration. When the business complies with the user configuration, corresponding event is triggered. The event detector sends an event notification to the smart management server.

- Smart management server

  A smart management server receives the event notification from the event detector and determines whether to trigger a policy based on the event. After the policy is triggered, the smart management server runs the policy in policy management.

- Policy manager

  A policy manager manages SEM policies and runs actions in the policies that are triggered by the smart management server.

- SEM environmental variable

  It indicates a variable that is used by an action of a policy during SEM running. There are three types of SEM environmental variables:

  - Global variable
  - Local system variable
  - Local user variable

  The words and signs located between the United States Dollar sign ($) and the first non-letter, non-digit, and non-underline character are used as the name of a variable to be replaced. Global variables can be used in all policies. Local system variables and local user variables are local variables and can be used in specific policies only. The local system variables are read-only. The local user variables are defined by the actions in the policies during policy running. Therefore, the local system variables start with the underline (_) to avoid confusion with the local user variables.

- Specific application event of SEM

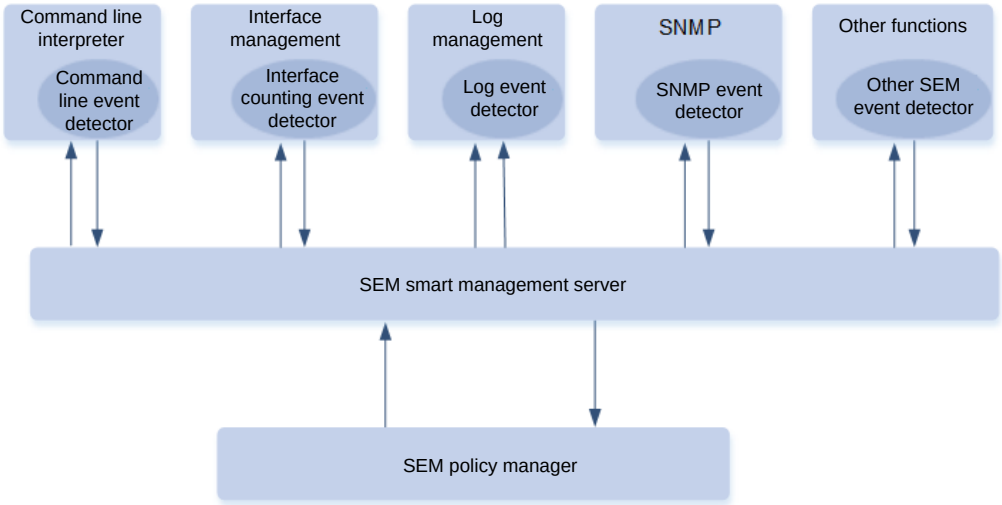
  SEM supports specific application events in the SEM system. These events are used to trigger a policy during running of another policy. Subsets and types are used to distinguish specific application events. Specific application events of SEM are detected by the specific application event detector based on subsets and types, and are released by their actions in the running policy. When an action in the running policy releases a specific application event of a subset and type, the detected event of the subset and type is triggered.

- SEM naming counter

  SEM supports a naming counter in the SEM system. Change in the SEM naming counter is detected by the counting event detector of SEM. The value of the SEM naming counter is operated by the counter action in the running policy. The SEM naming counter can be used for policy trigger counting and numerical statistics.

1.1.3 Principle

Figure 1-1 SEM Structure



As shown in Figure 1-1, SEM provides different types of event detectors. These events detectors are embedded in different business to monitor the business in real time. The detectors try to match event triggering conditions in user configurations with business running events. If a match is hit, the event detector notifies the smart management server of the event.

On the basis of the event configuration in the policy, the smart management server determines whether to trigger a policy to run. If the event triggering conditions are met, the smart management server runs the policy in the policy manager.

The policy in the policy manager runs preset actions in order based on user configuration.

1. Event Detectors Supported by SEM

SEM supports a variety of event detectors. These event detectors are embedded in different business. They detect the running business, and decide whether any event occurs. SEM supports the following detector types:

- Counting event detector

  The counting event detector detects the naming counter in SEM. When the naming counter exceeds the specified threshold, a counter event is triggered. After the counter event is triggered, the counting event detector stops working temporarily, and resumes until the counter reaches the threshold. The value of the naming counter is changed by the action of the running counter and can thus be accumulated by other policies. When the counter reaches a threshold, a counter event is triggered, which triggers the policy to run. During the running of this policy, the value of the counter is reset to realize circulation.

- Interface counting event detector

  The interface counting event detector detects interface statistics of a device. By periodic collection and statistics, the detector determines whether the statistics of an interface exceeds a threshold. If yes, an interface counting event is triggered. After the interface counting event is triggered, the interface counting event detector stops working temporarily and resumes until the interface counter reaches the recovery threshold or the suspension time exceeds the recovery cycle.

- Syslog event detector

  The syslog event detector detects log information of a device and uses regular expressions to match the log information. If the log information is matched using the regular expressions, a syslog event is triggered.

- Timer event detector

  The timer event detector detects time-related events.

  - Countdown timer event: The timer time is the number of seconds before which a policy takes effect. When the effective time reaches the number of such seconds, the timer event is triggered.

- Track event detector

  The track event detector detects tracks. Track refers to status change of a reliable network service (RNS). The track event detector detects change in the status of a tracked entity. When the status of a tracked entity changes, the track event is triggered.

2. Policy Actions Supported by SEM

SEM supports different actions. An action runs after a policy is triggered by an event. The actions include information collection and device/network troubleshooting. SEM supports the following actions:

- Run CLI commands: Run commands set by users.
- Send syslog: Send specified log messages.
- Operate naming counter: Operate the naming counter in SEM.
- Reset device: Reset devices.
- Wait during policy running: Wait for some time during policy running.
- Configure environmental variables: Configure local policy variables.

3. Management of the SEM Smart Management Server

The SEM smart management server provides management interfaces to allow users to view SEM running information and perform management. Users can view different types of SEM information, including:

- Supported detector types
- Versions of the smart management server and event detectors
- User configuration and submitted policies
- Event history
- Currently defined counter

1.2 Configuration Task Summary

SEM configuration includes the following tasks:

(1) Configuring SEM Policies

(2) (Optional) Configuring Parameters of SEM Policies

1.3 Enabling the SEM Function

1.3.1 Overview

SEM is separately deployed in a device independent from external network management tools. SEM allows customers to customize different types of events and policies so that customers can freely obtain or monitor their desired event information and actions taken for the events.

1.3.2 Restrictions and Guidelines

- The syslog function must be enabled by using the **logging** command before syslog actions are configured.
- The device must be equipped with a normal standby engine before actions are switched to the standby engine.
- Run the **action reload** command with caution. It may cause repeated restart of the system or repeated active/standby switchover.

1.3.3 Configuring SEM Policies

1. Overview

By configuring SEM policies, users can monitor events based on actual needs.

2. Restrictions and Guidelines

- When multiple events are configured for a policy, the events are automatically arranged in the alphabetical order of tags. You are advised to use the naming method based on a sequencing rule, for example, 01_cli, 02_timer, and 03_counter.
- The relationship between events refers to the relationship of the current event with the combination of all other events. Only when the first event is triggered, SEM checks whether to trigger a policy. If users try to configure juxtaposition for other events except the first event, the default juxtaposition is an AND relation. In this case, the juxtaposition of the first event is ignored.
- In either of the following scenarios, the **rollback** command can be used to roll back the policy configuration.
  - A new configured policy has not been submitted.
  - A configured policy has been submitted and registered, but changes to the policy have not been submitted.
- If no action is configured for a submitted policy, the policy can be registered. However, no action is taken when the policy is triggered.
- Generally, multiple actions are configured for a policy. When the policy is triggered, the actions are run in the alphabetical order of the *label* parameter.
- To save the I/O of CLI commands, run the **policy record** command.
  The **smart manager policy record** command does not save the command I/O as well.
- If the policy is being edited but is submitted, run the **list-config** command to display the configuration not submitted in the currently edited policy. The **commit** command is not included in the displayed content. If the policy is submitted, the configuration of the submitted policy is displayed. The **commit** command is included in the displayed content.
- The submittable policies are divided into new policies and edited and registered policies. When a registered

but unedited policy is not submitted, a notification will be displayed. If users want to quit the changes to the policy configuration before submitting the changes, run the **rollback** command to roll back the policy configuration.

- During submission, the validity of the policy configuration is checked. If the checking fails, the policy configuration fails to be submitted. In this case, the policy is not registered and remains in the editing status. For example, if no event is configured for the policy, the policy submission checking fails.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an SEM policy and enter the SEM configuration mode.

smart manager applet *applet-name*

No policy is configured by default.

(4) Configure events. Configure at least one of the following tasks.

- Configure a counter monitoring event.

  event tag *event-name* [**correlate** { **andnot** | **and** | **or** }] **counter name** *counter-name* **entry-op** *operator* **entry-val** *entry-value* **exit-op** *operator* **exit-val** *exit-value*

  No counter monitoring event is configured by default.

- Configure an interface monitoring event.

  event tag *event-name* [**correlate** { **andnot** | **and** | **or** }] **interface name** *interface-type interface-number* **parameter** { **link_up** | **link_down** }

  No interface monitoring event is configured by default.

- Configure a log monitoring event.

  event tag *event-name* [**correlate** { **andnot** | **and** | **or** }] **syslog pattern** *regular-expression* [**priority** *priority-level*] [**occurs** *num-occurrences*] [**period** *period-value*] [**skip** { **yes** | **no** }]

  No log monitoring event is configured by default.

- Configure a timer monitoring event.

  event tag *event-name* [**correlate** { **andnot** | **and** | **or** }] **timer**

  No timer monitoring event is configured by default.

- Configure a track monitoring event.

  event tag *event-name* [**correlate** { **andnot** | **and** | **or** }] **track** [**state** { **up** | **down** }] [*track-id*]

  No track monitoring event is configured by default.

A complete policy is composed of events and actions. If no event is configured for the policy, an error occurs during policy submission, resulting in submission failure.

(5) Configure actions. Configure one of the following tasks.

- Run CLI commands of a device.

  action *action-label* **cli command** *cli-string* [**pattern** *pattern-string*]

- Operate SEM counters.

  action *action-label* **counter name** *counter-name* **op** { **dec** | **inc** | **nop** | **set** } **value** *counter-value*

- Terminate a policy script and set the exiting status.

  action *action-label* **exit** [*result*]

- Restart the device.

  action *action-label* **reload**

- Set local variables.

  action *action- label* **set** *variable-name variable-value*

- Carry out logging.

  action *action-label* **syslog** [**priority** *priority-level*] **msg** *syslog-message* [**facility** *mnemonics*]

- Pause a policy script.

  action *action-label* **wait** *wait-time*

No action is configured by default.

(6) Enable the function of recording CLI action output.

policy record

The recording function is not enabled for CLI command action output by default.

(7) (Optional) Configure description.

description *string*

No description is configured for an SEM policy by default.

(8) (Optional) Display current policy configuration.

list-config

(9) (Optional) Roll back configuration.

rollback

(10) Submit configuration.

commit

1.3.4 Configuring Parameters of SEM Policies

1. Restrictions and Guidelines

Modification to policy description takes effect immediately without submission.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure upper limits of SEM parameters. Configure at least one of the following tasks.

- Configure the upper limits of SEM detector parameters.

  smart manager detector { **counter** | **interface** | **timer** } **event-number** *detector-number*

By default, the maximum number of events for the counting detector, the maximum number of events for the interface detector, and the maximum number of events for the timer detector are **256**, respectively.

- Configure the maximum number of SEM global variables.

  smart manager global-variant number *global-variant-number*

  By default, the maximum number of global variables is **512**.

- Configure the upper limits of SEM policy parameters.

  smart manager policy { **action-number** *policy-number* | **config-number** *policy-number* | **event-number** *policy-number* | **register-number** *policy-number* | **trigger-delay-number** *policy-number* }

  By default, the maximum number of actions in a policy is **64**; the maximum numbers of policy detectors and registered policies are **128**, respectively; and the maximum numbers of configured policies and policy delayed triggers are **256**, respectively.

- Configure the upper limits of SEM configuration instance parameters.

  smart manager record { **size-of-instance** *record-number* | **size-of-policy** *record-number* }

  By default, the maximum number of policy instances is **50** and the maximum size of a policy file is **1024** KB.

- Configure the upper limits of SEM scheduler parameters.

  smart manager schdulr { **pending-number** *schdulr-number* | **running-number** *schdulr-number* }

  By default, the maximum number of wait policies of the scheduler and the maximum number of policies run by the scheduler are **128**, respectively.

1.4 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-1 SEM Monitoring

Command	Purpose
show smart manager detector [**all** | *detector-name*] [**statistics**]	Displays SEM detector information.
show smart manager history events [**detailed**] [**maximum** *number*]	Displays SEM history information.
show smart manager policy all	Displays all policies and policy submission information.
show smart manager policy registered [**policy** *policy-name*] [**event-type** *event-name*] [**class** *class-options*] [**statistics**]	Displays information of registered policies.
show smart manager version	Display SEM versions.

1.5 Configuration Examples

1.5.1 Configuring an Interface Monitoring Event

1. Requirements

Device A is directly connected to Device B through GigabitEthernet 0/1. Due to the problem of the line or Device B, Device A often receives many consecutive error frames, which affects communication. After GigabitEthernet 0/1 of Device A is shut down and restarted, the problem is solved.

2. Topology

Figure 1-2 Topology of an Interface Monitoring Event

3. Notes

(1) Create a policy.

(2) Configure an interface monitoring event.

(3) Configure CLI command actions.

(4) Submit the policy configuration.

4. Procedure

(1) Create a policy with the name policy_interface on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA (config)# smart manager applet policy_interface
```

(2) Configure an event with the name event_1 in the policy_interface policy and set the type to interface. The specific parameter configuration is as follows:

Configure the interface counting type as link_down and set the interface status to down.

Configure the interface name as GigabitEthernet 0/1 to specify the interface to be detected.

```
DeviceA (sem-applet)# event tag event_1 interface name GigabitEthernet 0/1
parameter link_down
```

(3) Configure actions of the policy_interface policy.

Configure action_1 to run the **enable** command to enter the privileged EXEC mode.

```
DeviceA (sem-applet)#action action_1 cli command "enable"
```

Configure action_2 to run the **configure terminal** command to enter the global configuration mode.

```
DeviceA (sem-applet)#action action_2 cli command "configure terminal"
```

Configure action_3 to run the **interface GigabitEthernet 0/1** command to enter the interface configuration mode.

```
DeviceA (sem-applet)#action action_3 cli command "interface GigabitEthernet 0/1"
```

Configure action_4 to run the **no shutdown** command to set the interface status to up.

```
DeviceA (sem-applet)#action action_4 cli command "no shutdown"
```

(4) Submit the policy.

```
DeviceA(sem-applet)# commit
```

(5) Exit the policy editing status.

```
DeviceA(sem-applet)# exit
```

5. Verification

Run the **show smart manager policy registered** command to display a registered SEM policy.

```
DeviceA# show smart manager policy registered
 No.  Name                                                    Type    Event Type
   1  policy_interface                                          applet  interface
  event_1: interface: parameter link_down name GigabitEthernet 0/1
  action action_1 cli command "enable"
  action action_2 cli command "configure terminal"
  action action_3 cli command "interface GigabitEthernet 0/1"
  action action_4 cli command "no shutdown"
```

Run the **show smart manager policy active** command to display an active policy.

```
DeviceA# show smart manager policy active
Key: P - Priority       :L - Low, H - High, N - Normal
    S - Scheduling node :A - Active, P - Pending

No.  Job id   P S Status    Time Of Event       Event Type    Policy Name
1    2       N A suspend   2021-03-19 18:05:59  interface    policy_interface
```

Set GigabitEthernet 0/1 to the down status to verify whether the policy takes effect.

```
DeviceA# configure terminal
DeviceA (config)# interfce GigabitEthernet 0/1
DeviceA (config-if-GigabitEthernet 0/1)#shutdown
*Mar 19 18:06:19: %SEM-6-PLCY_TRG: Policy policy_1 id 2 is triggered by event 2, and
the policy instance id is 1.
```

Run the **show smart manager history events detailed** command to display SEM event history.

```
DeviceA# show smart manager history events detailed
No.     Job id   Event Type      Time                  Policy name
1       2       interface       2021-03-22 17:19:38      policy_interface
        Class: default, Policy Type: applet
```

6. Configuration Files

Device configuration file

```
hostname DeviceA
!
smart manager applet policy_interface
 event tag event_1 interface name GigabitEthernet 0/1 parameter link_down
```

```
 action action_1 cli command "enable"
 action action_2 cli command "configure terminal"
 action action_3 cli command "interface GigabitEthernet 0/1"
 action action_4 cli command "no shutdown"
!
end
```

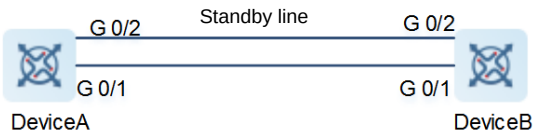
1.5.2 Configuring a Counter Monitoring Event

1. Requirements

Device A is directly connected to Device B through GigabitEthernet 0/1. A low-bandwidth standby line is created between Device A and Device B through GigabitEthernet 0/2. Due to the problem of the line or Device B, Device A often receives many consecutive error frames on GigabitEthernet 0/1, which affects communication. After GigabitEthernet 0/1 of Device A is shut down and restarted, the problem is solved. If the counter monitoring event is triggered more than 50 times, GigabitEthernet 0/1 is shut down permanently and the standby line is used.

2. Topology

Figure 1-3 Topology of a Counter Monitoring Event



3. Notes

(1) Configure an interface monitoring event, including interface counting event, CLI actions, and counter actions.

(2) Configure a counter monitoring event for detecting interface monitoring events.

4. Procedure

(1) Create a policy with the name policy_interface on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# smart manager applet policy_interface
```

(2) Configure an event with the name event_1 in the policy_interface policy and set the type to interface. The specific parameter configuration is as follows:

Configure the interface counting type as link_down and set the interface status to down.

Configure the interface name as GigabitEthernet 0/1 to specify the interface to be detected.

```
DeviceA (sem-applet)# event tag event_1 interface name GigabitEthernet 0/1
parameter link_down
```

(3) Configure actions of the policy_interface policy.

Configure action_1 to run the **enable** command to enter the privileged EXEC mode.

```
DeviceA (sem-applet)#action action_1 cli command "enable"
```

Configure action_2 to run the **configure terminal** command to enter the global configuration mode.

```
DeviceA (sem-applet)#action action_2 cli command "configure terminal"
```

Configure action_3 to run the **interface GigabitEthernet 0/1** command to enter the interface configuration mode.

```
DeviceA (sem-applet)#action action_3 cli command "interface GigabitEthernet 0/1"
```

Configure action_4 to run the **no shutdown** command to set the interface status to up.

```
DeviceA (sem-applet)#action action_4 cli command "no shutdown"
```

Configure action_5, and increase the value of the naming counter for the SEM policy name of policy_interface by 1.

```
DeviceA(sem-applet)# action action_5 counter name policy_interface op inc value
1
```

(4) Submit the policy.

```
DeviceA(sem-applet)# commit
```

(5) Exit the policy editing status.

```
DeviceA(sem-applet)# exit
```

(6) Create a policy with the name policy_counter.

```
DeviceA(config)# smart manager applet policy_counter
```

(7) Configure an event with the name event_counter in the policy_counter policy and set the event type to SEM counter. The specific parameter configuration is as follows:

Set the counter name to policy_interface, which is the policy name in step (1) .

Set the counter trigger parameter **entry-op ge entry-val** to **6**, indicating that the event is triggered when the value of the SEM counter is equal to or greater than 6.

Set the counter restoration parameter **exit-op gt exit-val** to **5**, indicating that event monitoring is restored immediately when the value of the SEM counter is greater than 5.

```
DeviceA(sem-applet)# event tag event_counter counter name policy_interface
entry-op ge entry-val 6 exit-op gt exit-val 5
```

(8) Configure actions of the policy_counter policy.

Configure action_counter_1 to set the value of the counter policy_interface to 0.

```
DeviceA(sem-applet)# action action_counter_1 counter name policy_interface op set
value 0
```

Configure action_counter_2 to run the **enable** command to enter the privileged EXEC mode.

```
DeviceA(sem-applet)# action action_counter_2 cli command "enable"
```

Configure action_counter_3 to run the **configure terminal** command to enter the global configuration mode.

```
DeviceA(sem-applet)# action action_counter_3 cli command "configure terminal"
```

Configure action_counter_4 to run the **interface GigabitEthernet 0/1** command to enter the interface configuration mode.

```
DeviceA(sem-applet)# action action_counter_4 cli command "interface
GigabitEthernet 0/1"
```

Configure action_counter_5 to run the **shutdown** command to set the interface status to down permanently.

```
DeviceA(sem-applet)# action action_counter_5 cli command "shutdown"
```

(9) Submit the policy.

```
DeviceA(sem-applet)# commit
```

(10) Exit the policy editing status.

```
DeviceA(sem-applet)# exit
```

5. Verification

Run the **show smart manager policy registered** command to display a registered SEM policy.

```
DeviceA# show smart manager policy registered
No.  Name                                                    Type    Event Type
   1  policy_interface                                        applet  interface
  event_1: interface: parameter link_down name GigabitEthernet 0/1
  action action_1 cli command "enable"
  action action_2 cli command "configure terminal"
  action action_3 cli command "interface GigabitEthernet 0/1"
  action action_4 cli command "no shutdown"
    policy record per-instance 50 per-policy 1000

   2  policy_counter                                          applet  counter
  event_counter: counter: name policy_interface entry-op ge entry-val 6 exit-op gt
exit-val 5
  action 1 counter name policy_interface op set value 0
  action action_counter_1 cli command "enable"
  action action_counter_2 cli command "configure terminal"
  action action_counter_3 cli command "interface GigabitEthernet 0/1"
  action action_counter_4 cli command "shutdown"
  action action_counter_5 cli command "end"
```

Set GigabitEthernet 0/1 to the down status five times. Run the **show smart manager detector** command to display the monitoring event information.

```
DeviceA# show smart manager detector counter statistics
detector counter events number: 1
    event id: 3, event name: event_counter
      counter name: policy_interface
      counter value: 5
      status: enable
      trigger times: 0
      trigger policy times: 0
```

Set GigabitEthernet 0/1 to down status again to trigger the policy_counter policy, and run the **show smart manager detector** command to display the monitoring event information.

```
DeviceA# show smart manager detector counter statistics
detector counter events number: 1
   event id: 3, event name: event_counter
     counter name: policy_interface
     counter value: 1
     status: enable
     trigger times: 1
     trigger policy times: 1
```

Run the **show smart manager history events detailed** command to display SEM event history.

```
DeviceA# show smart manager history events detailed
No.     Job id   Event Type      Time                   Policy name
1       65      interface       2021-03-24 11:27:30      policy_interface
        Class: default, Policy Type: applet
2       54      counter         2021-03-24 11:27:29      policy_counter
        Class: default, Policy Type: applet
3       64      interface       2021-03-24 11:27:29      policy_interface
        Class: default, Policy Type: applet
4       63      interface       2021-03-24 11:24:43      policy_interface
        Class: default, Policy Type: applet
5       62      interface       2021-03-24 11:24:41      policy_interface
        Class: default, Policy Type: applet
6       61      interface       2021-03-24 11:24:29      policy_interface
        Class: default, Policy Type: applet
7       60      interface       2021-03-24 11:24:25      policy_interface
        Class: default, Policy Type: applet
8       59      interface       2021-03-24 11:24:07      policy_interface
        Class: default, Policy Type: applet
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
smart manager applet policy_interface
 event tag event_1 interface name GigabitEthernet 0/1 parameter link_down
 action action_1 cli command "enable"
 action action_2 cli command "configure terminal"
 action action_3 cli command "interface GigabitEthernet 0/1"
 action action_4 cli command "no shutdown"
 action action_5 counter name policy_interface op inc value 1
!
smart manager applet policy_counter
 event tag event_counter counter name policy_interface entry-op ge entry-val 6 exit-op
gt exit-val 5
 action 1 counter name policy_interface op set value 0
 action action_counter_1 cli command "enable"
```

```
 action action_counter_2 cli command "configure terminal"
 action action_counter_3 cli command "interface GigabitEthernet 0/1"
 action action_counter_4 cli command "shutdown"
 action action_counter_5 cli command "end"
 commit
!
end
```

1.5.3 Configuring a Syslog Monitoring Event

1. Requirements

Though the interface status is down, Device A sends logs. When the logs are detected, the interface status must be restored to up.

2. Topology

Figure 1-4 Topology of a Syslog Monitoring Event

3. Notes

(1) Create a policy.

(2) Configure a syslog monitoring event.

(3) Configure actions.

(4) Configure policy trigger parameters.

(5) Submit the policy configuration.

4. Procedure

(1) Create a policy with the name policy_syslog on Device A.

```
Device> enable
DeviceA# configure terminal
DeviceA(config)# smart manager applet policy_syslog
```

(2) Configure an event with the name event_syslog1 in the policy_syslog policy, set the type to syslog, and put logs with the content "LINEPROTO-5-UPDOWN" within the detection scope.

```
DeviceA(sem-applet)# event tag event_1 syslog pattern "LINEPROTO-5-UPDOWN"
priority critical
```

(3) Configure an event with the name event_syslog2 in the policy_syslog policy, set the type to syslog, and put logs with the content "GigabitEthernet 0/1" within the detection scope.

```
DeviceA(sem-applet)# event tag event_syslog2 syslog pattern "GigabitEthernet 0/1"
```

(4) Configure an event with the name event_syslog3 in the policy_syslog policy, set the type to syslog, and put logs with the content "changed state to down" within the detection scope. The conditional relationship between event_syslog3 and event_syslog1/event_syslog2 is an AND relation.

```
DeviceA(sem-applet)# event correlate and tag event_syslog3 syslog pattern "changed
state to down"
```

(5) Configure actions of the policy_syslog policy.

Configure action_syslog_1 to run the **enable** command to enter the privileged EXEC mode.

```
DeviceA(sem-applet)# action action_syslog_1 cli command "enable"
```

Configure action_syslog_2 to run the **configure terminal** command to enter the global configuration mode.

```
DeviceA(sem-applet)# action action_syslog_2 cli command "configure terminal"
```

Configure action_syslog_3 to run the **interface GigabitEthernet 0/1** command to enter the interface configuration mode.

```
DeviceA(sem-applet)# action action_syslog_3 cli command "interface
GigabitEthernet 0/1"
```

Configure action_syslog_4 to wait for five seconds.

```
DeviceA(sem-applet)# action action_syslog_4 wait 5
```

Configure action_syslog_5 to run the **no shutdown** command to set the interface status to up.

```
DeviceA(sem-applet)# action action_syslog_5 cli command "no shutdown"
```

Configure action_syslog_6 to run the **end** command to exit the privileged EXEC mode.

```
DeviceA(sem-applet)# action action_syslog_6 cli command "end"
```

Configure action_syslog_7 to run the **show interfaces status | include UP** command to display the interface status.

```
DeviceA(sem-applet)# action action_syslog_7 cli command "show interfaces status
| include UP"
```

(6) Submit the policy.

```
DeviceA(sem-applet)# commit
```

(7) Exit the policy editing status.

```
DeviceA(sem-applet)# exit
```

5. Verification

Run the **show smart manager policy registered** command to display a registered SEM policy.

```
DeviceA# show smart manager policy registered
 No.  Name                                                    Type    Event Type
   1  policy_syslog                                            applet  syslog
  event_syslog1: syslog: pattern "LINEPROTO-5-UPDOWN"
  event_syslog2: syslog: pattern "GigabitEthernet 0/1"
  event_syslog3: syslog: pattern "changed state to down"
  action action_syslog_1 cli command "enable"
  action action_syslog_2 cli command "configure terminal"
  action action_syslog_3 cli command "interface GigabitEthernet 0/1"
  action action_syslog_4 wait 5
```

```
 action action_syslog_5 cli command "no shutdown"
 action action_syslog_6 cli command "end"
 action action_syslog_7 cli command "show interfaces status | include UP"
```

Run the **show smart manager policy active** command to display an active policy.

```
DeviceA# show smart manager policy active
Key: P - Priority       :L - Low, H - High, N - Normal
    S - Scheduling node :A - Active, P - Pending

No.  Job id   P S Status    Time Of Event       Event Type    Policy Name
1    10      N A suspend   2021-03-23 11:01:49  syslog       policy_syslog
```

Set GigabitEthernet 0/1 to the down status to verify whether the policy takes effect.

```
DeviceA# configure terminal
DeviceA(config)# interfce GigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)#shutdown
*Mar 23 11:02:03: %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to
administratively down.
*Mar 23 11:02:03: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1,
changed state to down.
*Mar 23 11:02:03: %SEM-6-PLCY_TRG: Policy policy_syslog id 7 is triggered by event
10, and the policy instance id is 12.
*Mar 23 11:02:11: %LINK-3-UPDOWN: Interface GigabitEthernet 0/1, changed state to up.
*Mar 23 11:02:11: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1,
changed state to up.
```

Run the **show smart manager history events detailed** command to display SEM event history.

```
DeviceA# show smart manager history events detailed
No.     Job id   Event Type      Time                   Policy name
1       10      syslog         2021-03-23 11:02:03      policy_syslog
        Class: default, Policy Type: applet
```

6. Configuration Files

```
hostname DeviceA
!
smart manager applet policy_syslog
 event tag event_syslog1 syslog pattern "LINEPROTO-5-UPDOWN"
 event tag event_syslog2 syslog pattern "GigabitEthernet 0/1"
 event correlate and tag event_syslog3 syslog pattern "changed state to down"
 action action_syslog_1 cli command "enable"
 action action_syslog_2 cli command "configure terminal"
 action action_syslog_3 cli command "interface GigabitEthernet 0/1"
 action action_syslog_4 wait 5
 action action_syslog_5 cli command "no shutdown"
 action action_syslog_6 cli command "end"
 action action_syslog_7 cli command "show interfaces status | include UP"
 commit
!
```

```
end
```

1.5.4 Configuring a Track Monitoring Event

1. Requirements

To facilitate management, a log is printed when the status of a specified or random tracked entity of Device A changes.

2. Topology

Figure 1-5 Topology of a Track Monitoring Event

3. Notes

(1) Create a policy.

(2) Configure a track monitoring event.

(3) Configure actions.

(4) Submit the policy configuration.

4. Procedure

(1) Create a policy with the name policy_track on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# smart manager applet policy_track
```

(2) Configure an event with the name event_track in the policy_track policy, set the type to track, and detect all tracked objects in the down status.

```
DeviceA(sem-applet)# event tag event_track track state down
```

(3) Configure actions of the policy_track policy.

Configure action_track1 to print "track obj down".

```
DeviceA(sem-applet)# action action_tarck1 syslog msg “track obj down.”
```

Configure action_track2 to run the **enable** command to enter the privileged EXEC mode.

```
DeviceA(sem-applet)# action action_track2 cli command "enable"
```

Configure action_track3 to run the **configure terminal** command to enter the global configuration mode.

```
DeviceA(sem-applet)# action action_track3 cli command "configure terminal"
```

Configure action_track4 to run the **interface GigabitEthernet 0/1** command to enter the interface configuration mode.

```
DeviceA(sem-applet)# action action_track4 cli command "interface GigabitEthernet
0/1"
```

Configure action_track5 to run the **no shutdown** command to set the interface status to up.

```
DeviceA(sem-applet)# action action_track5 cli command "no shutdown"
```

(4) Submit the policy.

```
DeviceA(sem-applet)# commit
```

(5) Exit the policy editing status.

```
DeviceA(sem-applet)# exit
```

(6) Configure a track monitoring event.

```
DeviceA(config)# track 1 Interface GigabitEthernet 0/1 line-protocol
DeviceA(config-track)# delay down 10
```

5. Verification

Run the **show smart manager policy registered** command to display a registered SEM policy.

```
DeviceA# show smart manager policy registered
No.  Name                                                    Type    Event Type
  1  policy_track                                             applet  track
  event_track: track: all state down
  action action_track1 syslog msg "track obj down"
  action action_track2 cli command "enable"
  action action_track3 cli command "configure terminal"
  action action_track4 cli command "interface GigabitEthernet 0/1"
  action action_track5 cli command "no shutdown"
```

Run the **show smart manager policy active** command to display an active policy.

```
DeviceA# show smart manager policy active
Key: P - Priority       :L - Low, H - High, N - Normal
    S - Scheduling node :A - Active, P - Pending

No.  Job id   P S Status    Time Of Event       Event Type    Policy Name
1    4       N A suspend   2021-03-22 17:21:49  track        policy_track
```

Set GigabitEthernet 0/1 to the down status to verify whether the policy takes effect.

```
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# shutdown
DeviceA(config-if-GigabitEthernet 0/1)# end
*Mar 22 17:21:59: %SEM-6-PLCY_TRG: Policy track id 4 is triggered by event 4, and the
policy instance id is 8.
*Mar 22 17:21:59: %SEM-6-COMM: track: track obj down
*Mar 22 17:22:01: %LINK-3-UPDOWN: Interface GigabitEthernet 0/1, changed state to up.
*Mar 22 17:22:01: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1,
changed state to up.
```

Run the **show smart manager history events detailed** command to display SEM event history.

```
DeviceA# show smart manager history events detailed
No.     Job id   Event Type      Time                  Policy name
1       4       track          2021-03-22 17:21:59      track
        Class: default, Policy Type: applet
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
smart manager applet policy_track
 event tag event_track track state down
action action_track1 syslog msg "track obj down"
 action action_track2 cli command "enable"
 action action_track3 cli command "configure terminal"
 action action_track4 cli command "interface GigabitEthernet 0/1"
 action action_track5 cli command "no shutdown"
commit
!
track 1 Interface GigabitEthernet 0/1 line-protocol
 delay down 10
!
end
```

Contents

1 Configuring Intelligent Monitoring 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Monitoring 1

1 Configuring Intelligent Monitoring

1.1 Introduction

1.1.1 Overview

Intelligent monitoring is an intelligent hardware management function of devices, including intelligent fan speed adjustment, and intelligent temperature monitoring. The intelligent monitoring function automatically adjusts fan speed based on the change of the ambient temperature, and monitors temperature change of the cards in real time in order to give notifications to users. By default, the intelligent monitoring function is enabled after the device is powered on. Users can use this function without need of any configuration. Apart from the default configuration, the system provides a variety of configuration methods so that you can change the default configuration of the system as necessary.

1.1.2 Principles

1. Power Monitoring

A device supports multiple power modules. However, different types of power modules cannot be mixed. When a power supply is inserted, the system identifies this power supply and checks whether it conflicts with the original power supply type. If yes, a power supply with a lower power is selected. The alarm indicator turns yellow and a log alarm is generated. After the power supply is removed, the abnormality is cleared and the system restores to normal.

2. Intelligent Speed Adjustment of Fans

The system automatically specifies a default start rotating speed for the fans based on the current operating mode of the fans. As the ambient temperature rises or drops, the fans automatically raise or reduce their rotating speed to dissipate heat and ensure that the noise is low.

3. Intelligent Temperature Monitoring

The active supervisor module monitors the temperature of all cards and notifies users of temperature change when the CA system runs normally.

1.2 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Figure 1-1 Monitoring

Command	Purpose
show fan [[[*device-id*] *fan-id*] **detail** | **version**]	Displays fan information.
show temperature	Displays line card information such as current temperature and temperature thresholds.

Command	Purpose
show power [**version**]	Displays power information about line cards and respective power supply priorities.

Contents

1 Configuring NETCONF 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Structure of NETCONF 1
1.1.3 NETCONF Session Interaction Procedure 2
1.1.4 Authentication Mechanism 9
1.1.5 Protocols and Standards 10
1.2 Configuration Task Summary 11
1.3 Configuring Communication Between the NETCONF Server and Client 11
1.3.1 Overview 11
1.3.2 Restrictions and Guidelines 11
1.3.3 Prerequisites 11
1.3.4 Procedure 11
1.4 Monitoring 12
1.5 Configuration Examples 13
1.5.1 Configuring NETCONF 13

1 Configuring NETCONF

1.1 Introduction

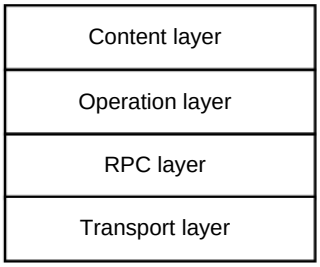
1.1.1 Overview

As network scale, complexity, and heterogeneity increase, it becomes more and more difficult for the traditional IP network management protocol Simple Network Management Protocol (SNMP) to manage the complicated network. In particular, SNMP cannot meet the requirements for configuration management and application system development of a large network. To overcome the shortcomings of SNMP, the Internet Engineering Task Force (IETF) formulates an extensible markup language (XML) based network management protocol – Network Configuration Protocol (NETCONF). NETCONF provides a programmable method to configure and manage network devices. This protocol configures parameters and obtains parameter values and statistics in XML packets and supports scalability, making network device configuration and management easy and efficient.

1.1.2 Structure of NETCONF

NETCONF supports the client/server (C/S) communication mode, in which a device runs the server of the protocol and a user runs the client of the protocol. NETCONF packets, including all configuration data and protocol messages, follow the XML format. With a hierarchical similarity to the ISO/OSI system, NETCONF consists of four layers from down to up: transport layer, remote procedure call (RPC) layer, operation layer, and content layer, as shown in Figure 1-1.

Figure 1-1 Structure of NETCONF



1. Transport Layer

The transport layer provides secure transmission channels for NETCONF and supports security protocols such as Secure Shell (SSH), Simple Object Access Protocol (SOAP), and Blocks Extensible Exchange Protocol (BEEP). Now, SSH is preferred.

2. RPC Layer

The RPC layer provides a simple transmission-irrelevant mechanism, including stipulations on the elements of error reply messages. RPC defines three message types:

- Hello: The hello messages are used to complete capability set exchange when a session is created between the NETCONF client and server.

- RPC and RPC-Reply: RPC are request messages sent by the NETCONF client to the NETCONF server, and RPC-Reply are reply messages returned by the NETCONF server to the NETCONF client. The reply messages are returned only when the NETCONF server receives RPC request messages; the reply messages and the received RPC request messages must contain the same message ID.
- Notification: The notifications are sent by means of subscription.

3. Operation Layer

Based on the basic primitive operation sets applied in RPC, 9 types of basic operation methods are defined:

- Data acquisition: Get and Get-Config
- Configuration: Edit-Config, Copy-Config, and Delete-Config
- Protection for critical resource (for example, configuration file) concurrency: Lock and Unlock
- Session ending: Close-Session and Kill-Session

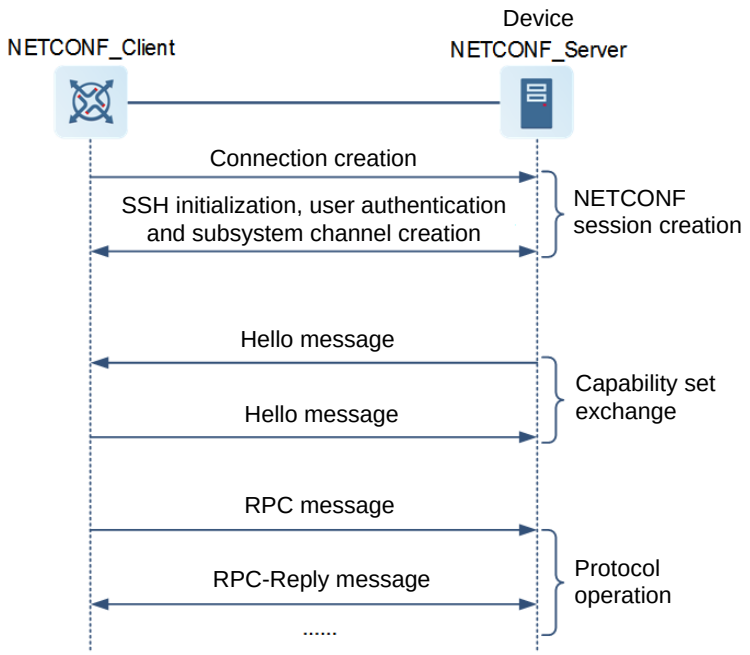
4. Content Layer

The content layer is a set of managed data objects. The content layer is the only layer that is not standardized and does not have a unified data model in NETCONF.

Note

Ruijie products use YANG for data modeling and XML for data transmission.

Figure 1-2 NETCONF Session Message Interaction



1.1.3 NETCONF Session Interaction Procedure

Figure 1-2 shows the NETCONF session interaction procedure, which falls into three parts.

1. Session Creation

(1) The transport layer of NETCONF relies on SSH. After the NETCONF server on a device starts the NETCONF process, a monitoring port is created.

(2) The NETCONF server monitors port 830 and creates an SSH channel. The SSH channel is created after a series of transport algorithm negotiations (including key agreement, compression algorithm, hash algorithm, encryption algorithm, and signature algorithm) and user authentication.

(3) After a session is created on the transport layer, the NETCONF client can exchange with the NETCONF server through this session.

Note

According to NETCONF, the default SSH TCP port ID is 830, which is customized based on the particular situation.

2. Capability Set Exchange

After the session is created, the NETCONF server and client send hello messages mutually to provide respective realized capability sets and ignore capabilities that are not understandable or realizable. The basic capability (urn:ietf:params:netconf:base:1.1) must be supported by the NETCONF server and client. To be compatible with earlier versions of NETCONF, the NETCONF server and client must support the basic capability (urn:ietf:params:netconf:base:1.0) of the earlier versions of NETCONF The NETCONF server and client finally obtain the intersected capabilities to perform subsequent data operation and management.

Caution

- In addition to the exchange capabilities defined in NETCONF RFC, developers can design other capabilities based on the specifications and formats described in NETCONF RFC.
- Capability exchange messages sent by the NETCONF client to the NETCONF server do not contain the session ID node (<session-id>).

3. Protocol Operation

- Get: Obtains device status or configuration data.

The packets sent by the client follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get>
<filter type="subtree">
      Configuration data (or status data) filtering rule
</filter>
</get>
</rpc>
```

The replies returned by the server follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
```

```
Obtained configuration data (or status data)
</data>
</rpc-reply>
```

If all subsets of status data on the device fail to match the filtering rule, an empty data node is returned as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="Message ID "
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
</rpc-reply>
```

- Get-config: Obtains configuration data based on the filtering node.

The packets sent by the client follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-config>
<source>
<running/>
</source>
<filter type="subtree">
     Protocol-based filtering rule
</filter>
</get-config>
</rpc>
```

The replies returned by the server follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
Obtained configuration data
</data>
</rpc-reply>
```

If all subsets of configuration data on the device fail to match the filtering rule, an empty data node is returned as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
</rpc-reply>
```

Note

The Get-config operation can obtain configuration data subsets through different subtree filtering rules but cannot obtain device status.

- Edit-config: Configures a device based on the model definitions and operation attributes.

In the edit-config packet, there are five operation attributes which are given in the description of the operation attribute of the XML packet. These five attributes are as follows:

- Merge: Merges the configuration data that includes this attribute in the Edit-config packets to the specified configuration file or database. If this configuration data does not exist, create this configuration data.
- Replace: Replaces the configuration data node in the specified configuration file or database with the configuration data that includes this attribute in the Edit-config packets. If this configuration data does not exist, create this configuration data based on the delivered content.
- Create: Creates configuration data that includes this attribute in the Edit-config packets in the specified configuration file or database. If the configuration data does not exist, deliver content to create this configuration data. If the configuration data exists, a reply, corresponding to the RPC-error packet, is returned and contains the value of error-tag "data-exists".
- Delete: Deletes configuration data that includes this attribute in the Edit-config packets from the specified configuration file or database. If the configuration data does not exist, a reply, corresponding to the RPC-error packet, is returned and contains the value of error-tag "data-missing". If the configuration data exists, corresponding configuration is deleted.
- Remove: Removes configuration data that includes this attribute in the Edit-config packets from the specified configuration file or database. If the configuration data does not exist, this operation is ignored and OK is returned. If the configuration data exists, corresponding configuration is removed.

The packets sent by the client follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<edit-config>
<target> <running/> </target>
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      Configuration data
</config>
</edit-config>
</rpc>
```

The replies returned by the server follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="Message ID "
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/>
</rpc-reply>
```

The Edit-config packet includes the Error-option node. The values of the Error-option node are of the enumerated type, including:

- **Continue-on-error**: During an Edit-config operation, if a configuration error occurs, the current error node is recorded and configuration continues. But an error message is returned finally (In the case of any configuration error, the final reply message is RPC-error).
- **Stop-on-error**: This is the default value of the Error-option. During an Edit-config operation, if a first configuration error occurs, the Edit-config operation stops immediately. The data configured before this error occurs takes effect.

The packets generally follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<edit-config>
<target> <running/> </target>
Acton option when a configuration error occurs
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      Configuration data
</config>
</edit-config>
</rpc>
```

Specification

Currently, Ruijie devices do not support the Replace operation. If this operation is delivered, it is processed as a Merge operation.

Note

- If the Edit-config packet does not include the error-option node, the default value of the error-option node is stop-on-error. Once a configuration error occurs on a node, the remaining configuration in the Edit-config packet stops immediately and an RPC-error is returned.
- If the Edit-config packet does not include the test-option node, the default value of the test-option node is **test-then-set**.
- If the Edit-config packet does not include the default-operation node, the default value of the default-operation node is **merge**.

- Copy-config: Copies the configuration file. For example, candidate configuration is copied to the configuration file, startup configuration is copied to the running configuration file, and running configuration is written into the startup configuration file. The copies can be successful if the target files support the write capability.

The packets sent by the client follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx"  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <copy-config>
    <target>
      <startup/>
    </target>
    <source>
      <running/>
    </source>
  </copy-config>
</rpc>
```

The replies returned by the server follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx"  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
```

```
  <ok/>
</rpc-reply>
```

- Delete-config: Deletes the configuration file. It is not allowed to delete the running file.

The packets sent by the client follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <delete-config>
   <target>
     <startup/>
   </target>
 </delete-config>
</rpc>
```

The replies returned by the server follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

Specification

Now, only the startup configuration can be synchronized to the running configuration file.

- Lock: Locks the configuration file. The configuration file can be accessed or modified through the current client, but cannot be accessed or modified by other clients or non-NETCONF clients (for example, SNMP or CLI). The packets sent by the client follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <lock>
   <target>
     <running/>
   </target>
 </lock>
</rpc>
```

The replies returned by the server follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx "  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

Note

According to RFC6241, the Lock operation is used to lock the configuration database (configuration files) and prevent multiple sources (for example, CLI, SNMP, and NETCONF sessions) from concurrently revising the configuration files. This avoids introducing other irrelevant configuration revisions. The device simplifies this operation, and can only prevent concurrent modifications (running configuration) from multiple NETCONF.

- Unlock: Unlocks the configuration database (configuration file, which indicates the running configuration file in a device). This operation is opposite to the Lock operation.

The packets sent by the client follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx "  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <unlock>
   <target>
     <running/>
   </target>
 </unlock>
</rpc>
```

The replies returned by the server follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx "  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

- Close-session: Closes the current session, including resource and lock release and disconnection.

The packets sent by the client follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <close-session/>
</rpc>
```

The replies returned by the server follow the format below:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx"  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

Note

Before the Close-session operation closes the current session, ensure that proceeding business has been completed and no new business request is received.

- Kill-session: Forcibly closes the current session, including resource and lock release and disconnection.

Caution

- Before using the Kill-session operation to forcibly close the current session, ensure that proceeding business has been stopped and unfinished business is rolled back to original state.
- The Kill-session operation cannot close the current session.

1.1.4 Authentication Mechanism

The NETCONF authentication mechanism is used to manage the NETCONF operations of specific users and the access to NETCONF resources, allowing the users to perform operations and access data nodes stipulated by NETCONF.

1. Access Permissions Supported by the NETCONF Authentication Mechanism

The NETCONF authentication function is not configured by default. Therefore, legal users have all NETCONF permissions. Access permissions supported by the NETCONF authentication mechanism are as follows:

- Create: Permits or denies new data nodes to be added.
- Read: Permits or denies data nodes to be read.
- Update: Permits or denies data nodes to be updated.
- Delete: Permits or denies data nodes to be deleted.
- Execute: Permits or denies all protocol operations.

2. Content Supported by the NETCONF Authentication Mechanism

The NETCONF authentication function supports RPC method authentication and data node authentication.

- RPC method authentication

  RPC method authentication of NETCONF is used to control permissions of the operation methods stipulated by NETCONF. Table 1-1 lists the RPC methods and default permissions.

Table 1-1 RPC Methods and Default Permissions

RPC Method	Function	Default Permission (R: read; W: write; X: execute)
get	Obtains data.	X→R
get-config	Obtains configuration.	X→R
edit-config	Edits configuration.	X→W
copy-config	Replaces the target configuration with the source configuration.	X
delete-config	Deletes configuration.	X
validate	Performs syntax check.	X
commit	Validates the candidate configuration and runs the configuration.	X
cancel-commit	Cancels the confirmed-commit operation.	X
discard-changes	Discards candidate configuration that has not taken effect.	X
lock/unlock	Locks or unlocks configuration.	X

RPC Method	Function	Default Permission (R: read; W: write; X: execute)
close-session	Closes the current session.	X
kill-session	Closes other sessions.	X
get-schema	Obtains the YANG file.	X

Note

- All RPC methods require the execution permission by default. The Get, Get-config, and Edit-config methods require the check of read/write permission for the data node.
- The Close-session method is permitted by default and cannot be denied.
- The Delete-config and Kill-session methods are denied by default, and can be configured as Permitted. Other RPC methods are permitted by default.
- The Lock and Unlock methods must be paired. If the Lock permission is configured, the Unlock permission is available as well.

- Data node authentication

  Data node authentication of NETCONF is used to control permissions of NETCONF data nodes. It can control the permissions of all modules, single module, and specific data nodes.

  - If only the slash (/) is configured, the authentication of NETCONF can control the permissions of the data nodes of all modules.
  - If a module name is configured, for example, /rg-snmp:snmp, the authentication of NETCONF can control the permissions of the data nodes of the single module.
  - In other configuration conditions, permission control is applied to the data nodes of specific modules.

1.1.5 Protocols and Standards

- RFC4741: NETCONF Configuration Protocol
- RFC4742: Using the NETCONF Configuration Protocol over Secure Shell (SSH)
- RFC4743: Using NETCONF over the Simple Object Access Protocol (SOAP)
- RFC4744: Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP)
- RFC5277: NETCONF Event Notifications
- RFC5381: Experience of Implementing NETCONF over SOAP
- RFC5539: NETCONF Over Transport Layer Security (TLS)
- RFC5717: Partial Lock RPC for NETCONF
- RFC6022: NETCONF Monitoring Schema
- RFC6241: Network Configuration Protocol
- RFC6242: Using the Network Configuration Protocol over Secure Shell
- RFC6243: With-defaults capability for NETCONF
- RFC6470: NETCONF Notification Events

- RFC6536: NETCONF Access Control Model (NACM)

Note

RFC4741 and RFC4742 have been replaced by RFC6241 and RFC6242 respectively.

1.2 Configuration Task Summary

NETCONF configuration includes the following tasks:

(1) Configuring Communication Between the NETCONF Server and Client

1.3 Configuring Communication Between the NETCONF Server and Client

1.3.1 Overview

After the NETCONF function is enabled on the NETCONF server, the NETCONF server can communicate with the NETCONF client to manage network devices.

1.3.2 Restrictions and Guidelines

- The **netconf yang multi-revision** command must be configured before the capability packet (Hello packet) of the NETCONF server is advertised.
- The **no netconf yang multi-revision** command must be configured before the capability packet (Hello packet) of the NETCONF server is advertised and one YANG module can advertise only its current latest version in the capability notification packet.
- In strict check mode, some XML packets that can be delivered in lightweight check mode may be intercepted.

1.3.3 Prerequisites

The NETCONF protocol is based on the SSH protocol. Before the NETCONF protocol is enabled, the SSH protocol must be configured. For the configuration procedure, see "Configuring SSH".

1.3.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the attribute parameters of the NETCONF server. The configuration tasks below are optional. Select tasks as required.

- (Optional) Enable the NETCONF service.

  netconf enable

  The NETCONF function is enabled by default.

- (Optional) Configure the maximum number of session connections supported by NETCONF.

netconf max-sessions *max-sessions-numbers*

The maximum number of session connections supported by NETCONF is **5** by default.

- (Optional) Configure the timeout time of the Edit-config operation in a NETCONF session.

  netconf timeout *timeout*

  The default timeout time of the Edit-config operation in a NETCONF session is **120** seconds.

- (Optional) Enable the YANG module multi-version notification function.

  netconf yang multi-revision

  The YANG module multi-version notification function of NETCONF is enabled by default.

- (Optional) Configure the NETCONF capabilities.

  netconf capability{ **candidate** | **rollback** | **validate** }

  The NETCONF-related capabilities are not configured by default.

- (Optional) Configure the NETCONF check mode.

  netconf calibration-mode { **lightweight** | **strict** }

  The default NETCONF check mode is lightweight check.

- (Optional) Enable the NETCONF logging function.

  netconf log { **capability** | **edit** | **get** | **session** }

  The NETCONF logging function is disabled by default.

- (Optional) Configure the port ID of the NETCONF server.

  netconf port *port-number*

  The default port ID of the NETCONF server is 830.

1.4 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-2 Monitoring

Command	Purpose
show netconf authorization user-name *name* { **rule-list** [**detail**] | **user-group** }	Displays a rule list that users are associated with, list details, and user group information.
show netconf session	Displays all session information of NETCONF.
show netconf statistics	Displays global statistics of NETCONF.
show netconf yang file	Displays all YANG files supported currently.
show netconf yang node-path	Displays all node paths supported currently.
show netconf yang tree	Displays all YANG model trees supported currently.

1.5 Configuration Examples

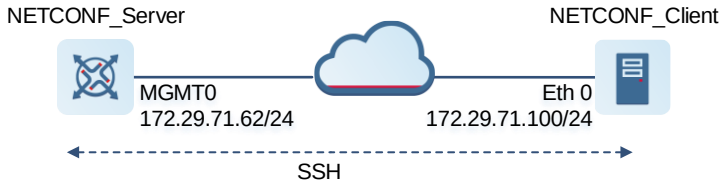
1.5.1 Configuring NETCONF

1. Requirements

NETCONF can be used as a network management tool to meet the high security and scalability requirements for network device management. NETCONF is based on SSH. As a security protocol of the application layer, SSH ensures security of NETCONF. As shown in Figure 1-3, the NETCONF network management software is used to manage and monitor network devices.

2. Topology

Figure 1-3 NETCONF Topology



3. Notes

- Configure an IP address for the network management interface of the NETCONF server to ensure that the NETCONF server and client are mutually reachable via L3 routes.
- Enable the SSH function on the NETCONF server.
- Configure NETCONF related parameters on the NETCONF server to meet requirements of actual scenarios.
- Connect the NETCONF server to the NETCONF client through SSH to manage and monitor network devices.

4. Procedure

Configure an IP address for the network management interface of the NETCONF server.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface mgmt 0
Hostname(config-if-Mgmt 0)# ip address 172.29.71.62 255.255.255.0
Hostname(config-if-Mgmt 0)# gateway 172.29.71.1
```

Enable the SSH function and generate a local key. For more information about the rule of selecting a key type, see the Usage Guidelines in the **crypto key generate** command in "SSH Commands".

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# enable service ssh-server
Hostname(config)# crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:y
```

```
Choose the size of the rsa key modulus in the range of 512 to 2048
and the size of the dsa key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
Choose the size of the ecc key modulus from (256, 384, 521)

How many bits in the modulus [1024]:2048
% Generating 2048 bit RSA1 keys ...[ok]
% Generating 2048 bit RSA keys ...[ok]
Hostname(config)#
```

Create an SSH user with the username **netconf** and set the password to netconf_1234.

```
Hostname(config)# username netconf privilege 15 password netconf_1234
```

Caution

To ensure security, you are advised to regularly modify the username and password.

Configure local user authentication of a VTY line.

```
Hostname(config)# line vty 0 35
Hostname(config-line)# login local
```

Enable the NETCONF service on the NETCONF server.

```
Hostname(config)# netconf enable
```

Set the maximum number of session connections supported by the NETCONF server to 6.

```
Hostname(config)# netconf max-sessions 6
```

Set the timeout time of the Edit-config operation in a NETCONF session to 100 seconds on the NETCONF server.

```
Hostname(config)# netconf timeout 100
```

Enable the YANG module multi-version notification function on the NETCONF server.

```
Hostname(config)# netconf yang multi-revision
```

Enable the candidate capability on the NETCONF server.

```
Hostname(config)# netconf capability candidate
```

Configure the check mode as lightweight check on the NETCONF server.

```
Hostname(config)# netconf calibration lightweight
```

Enable the syslog function related to the NETCONF sessions on the NETCONF server.

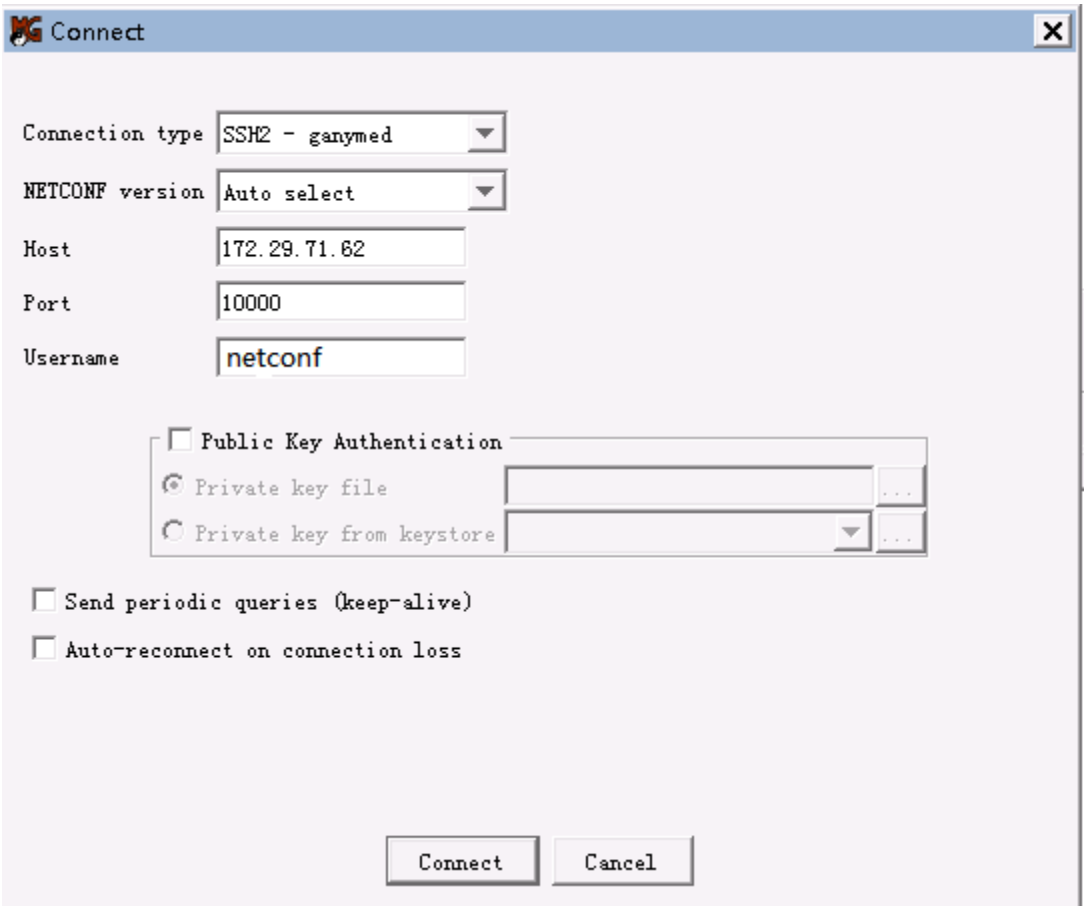
```
Hostname(config)# netconf log session
```

Set the port ID of the NETCONF service to 5000 on the NETCONF server.

```
Hostname(config)# netconf port 5000
```

Log in to the NETCONF server through the SSH protocol by using the NETCONF client software and manage and monitor network devices, as shown in Figure 1-4.

Figure 1-4 Device Login Example Through the NETCONF Client Software



5. Verification

Run the **ping** command to check whether the NETCONF server and client are mutually reachable via L3 routes.

```
Hostname# ping oob 172.29.71.100
Sending 5, 100-byte ICMP Echoes to 172.29.71.100, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms.
Hostname#
```

Run the **show service** command to check whether the SSH service is enabled.

```
Hostname# show service
snmp-agent    : enabled
ssh-server    : enabled
telnet-server : enabled
```

Run the **show netconf session** command to check whether the NETCONF server is connected to the NETCONF client software through the SSH protocol.

```
Hostname# show netconf session
************************session information***********************
                      Session count: 1
```

```
*********************************************************************
Session ID            : 20
Session version        : 1.1
Session transport      : netconf-ssh
Session login IP       : 172.29.69.21
Session login time     : 2020-12-18T08:26:30Z
Session in rpcs        : 0
Session in bad rpcs    : 0
Session out rpc errors  : 0
Session out notification: 0
Session out rpcs       : 0
Session out send fail   : 0
Session get           : 0
Session get config     : 0
Session edit config    : 0
Session copy config    : 0
Session delete config   : 0
Session close session   : 0
Session unsupport      : 0
Session lock_or_unlock  : 0
=====================================================================
```

6. Configuration Files

NETCONF_Server configuration file

```
hostname Hostname
!
username netconf privilege 15 password netconf_1234
!
netconf log session
netconf capability candidate
netconf port 5000
netconf max-sessions 6
netconf timeout 100
!
enable service ssh-server
!
interface Mgmt 0
 ip address 172.29.71.62 255.255.255.0
 gateway 172.29.71.1
!
line vty 0 35
 login local
!
end
```